UNIVERSITÀ DI CAGLIARI

Dipartimento di Ingegneria Elettrica ed Elettronica

Dottorato di Ricerca

Ph.D Thesis

Vitality detection in personal authentication systems using fingerprints

Ing. Pietro Coli

Advisor: Prof. Fabio Roli

Contents

Introduction

Fingerprints have always been an identification mean due to their some important properties: universality (everyone have one), permanence in the time (they do not change when the time passes), individuality (there are no two identical fingerprints). From the first forensic applications to the last biometric technology applied to access control, fingerprints are considered as the sign of each human being. The development of these biometric systems is driven by the intrinsic security of fingerprint (there is nothing to remember, like passwords or PINs, there is nothing to carry, like a card). But in 2002 an important vulnerability has been shown: it is possible to deceive fingerprint scanners through artificial replicas of fingertips. Several studies, using different materials, have demonstrated that all tested scanners (based on different physical principles) are not able to recognize fake to live fingertips. Considering that biometry was born specifically for secure applications, the risk of deceiving such systems by means of a synthetic clone of fingerprint has caught the attention of many academic and commercial groups. In order to address this shortcoming it is need to recognize a spoofing attempt with artificial fingers looking for some life signs each time an user submit a fingerprint: since the problem is to detect such signs, it is often referred as fingerprint vitality detection problem. Although this research field is still in its infancy, several

methods have been proposed so far, based on additional hardware to the existing capture device (detecting heartbeat, blood pressure etc.) and also on fingerprint image processing for extracting those life sign from the image captured by the sensor. The first goal of this Ph.D. thesis has been to investigate the current state-of-the-art in fingerprint vitality detection. Since the state-of-the-art is lack of a systematic classification of all the current methods, we arranged the above hardware-based and software-based approaches into a specific taxonomy on the basis of the sensing methodology or the physical phenomenon which is considered as a life sign (elastic deformation, perspiration or morphology of the skin). We also compared the performance of each fingerprint vitality detection approach and coupled our experimentation with results reported in the reference papers. The second contribution of this Ph.D. thesis is the development of two different new approaches, which we indicated as power spectrum and ridge-width fingerprint vitality detection. The former is based on 2D-Fourier Transform of the fingerprint image aimed to detect vitality signs in the frequency domain (we have found that high frequencies have a noteworthy importance in vitality detection). The latter is based on some morphological considerations in the space domain (intra-distance ridges and ridge width). Both approaches showed a promising performance, and, in particular, power spectrum features outperformed state-of-the-art methods. Experiments have been carried out on a dataset of images of live fingers and fake stamps collected at the DIEE laboratory in Cagliari (82 live fingers and 72 fake stamps, 20 acquisition for each finger/stamp). The dataset has been conceived for satisfying the requirements of all vitality measures (different impressions for static feature, different frames for dynamic ones). To the best of our knowledge, this is the largest data set for fingerprint vitality detection, and it has been made

publicly available into the research community, since, in our opinion, it can be considered a significant benchmark for fingerprint vitality detection approaches. Although vitality detection problem is far from its final solution, we believe this Ph.D. thesis contributed to a first interpretation key of all the current methods and to innovative proposals in fingerprint vitality detection. In the first chapter an introduction of biometric technology is shown with a closer examination of fingerprint biometric systems, the second chapter reviews all the main threats of a real systems from acquisition stage to storage data. Among all these vulnerabilities the biometric spoofing attacks are dealt in the third chapter. Chapter four deals with "liveness detection" methods from a review of the current methods to the newest approaches, arranged in a clear taxonomy tree. Chapter five and six presents our contribution in the field of liveness detection methods: from an experimentation on the main software based solutions we show, in chapter five, the different accuracy properties of the previous methods. In particular we focus on the effect of the fusion of complementary static and dynamic features. In the last chapter we give the results of liveness detection based on two morphologic feature: one based on ridge-width in the space domain, the other based on the study of high frequencies in the Fourier domain.

Chapter 1

Biometric systems

1.1 Identification and biometric data

At the end of the eighteenth century in the laboratory of the French police, Alphonse Bertillon gave the basis to the new forensic anthropology. This new methodology was based on some physical measures. Although the limited validity in the time of this approach (at the begin of nineteenth this method was rejected from juridical quarrel), we have to consider the effective importance of the idea. The essence of this method was the complete correspondence between the collected data of the anthroposomatic measures and the identity of a person. All the classified individuals are characterized completely only by some numbers referred to somatic marks, until this time criminals could be identified only based on eyewitness unreliable accounts. In 1882 Bertillon presented a criminal identification system known as ”anthropometry” and later also known as *Bertillonage*. In this system a person was identified by a set of measurements of the head and the whole body. The system was widely applied by French police and soon in other European coun-

tries. This method was a fundamental step in forensic science because for the first time the recognition of a person was based on a systematic approach. Although this revolutionary aspect, the Bertillonage was affected by numerous vulnerabilities: both the acquisition of the data (physical measures) and the matching process were carried out by human hand, with its intrinsic error and its subjectivity. All these limits caused in 1903 a relevant miscarriage of justice: in U.S. Penitentiary at Leavenworth, Kansas, two identical twins were confused each other because of their near anthropometric measures. This signed the end of *Bertillonage* and the begin of new identification approach.

1.2 Automatic systems for human recognition

The modern biometry is the study of methods for uniquely recognizing humans based upon one ore more intrinsic physical or behavioral traits. If we compare this last sentence with the Bertillon's method we can observe an evident resemblance. A biometric system is an automatic recognition process from some physics data to the identity of a person. Earlier this recognition process was assigned to the user who submitting a password or a smart card to an access control systems obtained the permission to enter in a secure place. The identity of a person was stored in something to remember (a password) or in something to have (a smart card): both this technologies have important limits (i.e. a password can be forgotten, or a smart-card can be lost). With biometric technology an access control systems recognizes automatically a person through his/her appearance or through some particular physilogical/physics elements. With this new approach the identity of a person is stored in the person.

In biometric technology a first important distinction must be done basing on the recognition modality:

- An *identification* process determines a person's identity by performing matches against multiple biometric templates. This type of systems is designed to determine identity based solely on biometric information. An Identification system answers the question "Who am I ?".

- A *verification/authentication* process is a one-to-one comparison in which the biometric system attempts to verify an individual's identity. In this case the captured biometric is compared with a previously stored template starting from a common user-id. The system receives as input both a biometric and an identification data. The verification answers the question "Is this the person who he/she claims to be ?".

Moreover, It is possible to distinguish wide range of biometric system technologies basing on the object of the measure: *physiological* systems are related to the shape of the body or a part of it, or to some physics characteristics; *behavioral* systems are related to the behavior of a person or to the way of doing something.

This is a brief overview of the main *physiological data*-based systems:

- **Face**: The face is the more common and more natural identification method. The acquisition of a face is done by a digital camera that records the front profile of the head of the user. At the moment these systems are affected by lighting condition, facial expression, aging etc.. In order to overcome this limit and improve the recognition accuracy new acquisition methodologies are developed: by the mean of a 3D scanner the whole face surface is

recorded, this measure offers more defined information than bidimensional acquisition of a camera and a complete invariance against light or context conditions.[1]-[2]-[3]

- **Infrared Thermograms**: The use of a IR source for the acquisition of a face or of an entire body can reveal something univocal traits of the person. Another advantage of the use of IR light is the robustness to different illumination conditions. In some systems the IR is employed to record the path of the veins under the skin of a body.[4]-[5]

- **Ear**: The shape of an ear can be distinctive for the identification of a person. By the extraction of some salient points from the ear-image and the computation of the ”intra-distances”, it is possible to quantify the degree of similarity among two ears.[6]-[7]

- **Hand Geometry**: Placing the hand on a flat scanner the system acquires some geometrical information by the user. The importance of this technology is the representation requirements: less than 10 bytes can be associated to each hand. Due to its limited distinctiveness this biometric datum is used only in some particular applications.[8]

- **Retinal scan**: In the last year in Holland a new national identification program has began for the regularization of the immigration by the scanning of the retinal vascularity of the eye. The image acquisition involves cooperation of the user.[9]-[10]

- **Iris**: The iris is a muscle of the eye that regulates the quantity of the light that reaches the retinal surface. The disposition of the fiber and its color

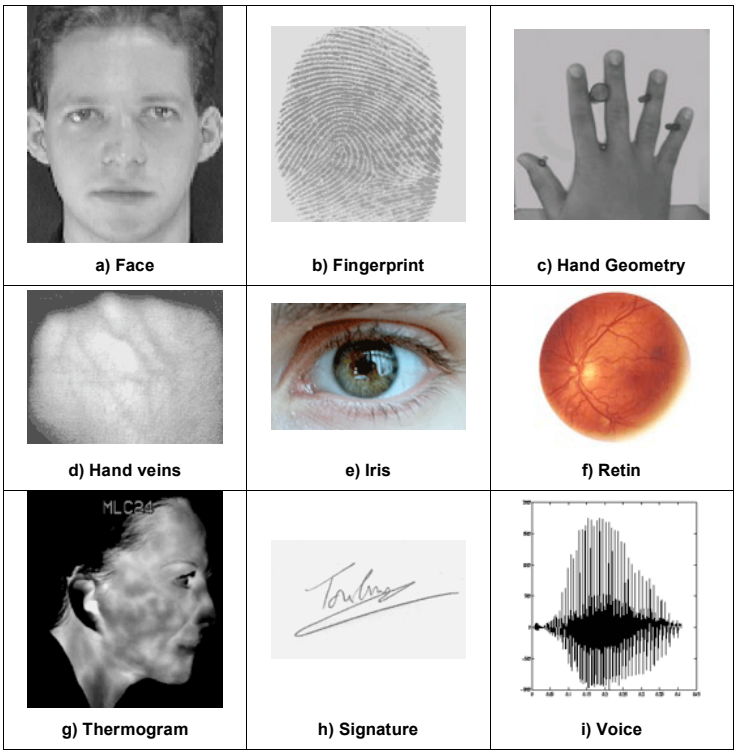


Figure 1.1: Biometric systems

makes a uniquely pattern for each person. The iris recognition technology is believed to be extremely accurate and fast.[11]

- **Fingerprint**: The oldest instrument for the forensic laboratory of identification. The flow of the papillary ridge under fingertip surface is a unique pattern for each person. Next section of this Ph.D. thesis is dedicated to this biometric.[20]

Some *behavioral data*-based systems are:

- **Gait**: The particular way of walking of each person encloses a significant biometrical trait. The speed, the length of a step, the movement of legs and

other measures are the salient data for a recognition process.[12]-[13]

- **Signature**: The way a person signs his name is known to be a characteristics of that individual. Signatures are behavioral biometrics that change over a period of time and are influenced by physical and emotional conditions.[14]

- **Keystrokes dynamics**: The rhythm of each person of writing with a keyboard can represent each individual. This technique is non invasive and can be monitored unobtrusively as a person is keying.[15]

1.3 Fingerprint and biometric systems

Among all the biometric systems, fingerprint-based identification is the most employed for commercial or forensic applications. The principal use of fingerprint is in the forensic laboratory where this biometric is considered as an evidence element in a crime scene. A fingerprint is the ridge flow left after that a fingertip touch a surface: the physiological wetness on the human skin is deposited on the surface reproducing the conformation of the papillary ridge. Each person leaves his/her own signature each time touches something, and this natural ”signature” is used to find the identity. In the following, we retrace the history of this important identification mean.

1.3.1 Fingerprint history

If we consider the use of fingerprint as an identification mean we can observe that there is no clear date when fingerprinting was first used. [18].
Fingerprint traces go back to ancient age: picture writing of a hand with ridge pat-

terns was discovered in Nova Scotia. In ancient Babylon, fingerprints were used on clay tablets for business transactions. In ancient China, thumb prints were found on clay seals. In 14th century, in Persia, several official government documents had fingerprints (impressions), and one government official observed that all the fingerprints are different.

In 1823, John Evangelist Purkinje, a professor of anatomy at the University of Breslau, published his thesis describing 9 fingerprint patterns. In this work there was not mention to fingerprint as an identification mean.

During the 1870, Dr. Henry Faulds, a British surgeon in Tokyo, faced the study of ”skin-furrows” after noticing finger marks on specimens of ”prehistoric” pottery. In 1880, Faulds gave an explanation of his classification system and a sample of the forms he had designed for recording inked impressions.

Sir Francis Galton, a British anthropologist and cousin of Charles Darwin, began his observations of fingerprints as a means of identification in the 1880's. At the end of nineteenth century Juan Vucetich, an Argentine Police Official, exploited for the first time Galton pattern types in fingerprint classification.

In 1900 the United Kingdom Home Secretary Office conducted an inquiry into ”Identification of Criminals by Measurement and Fingerprints.” Mr. Edward Richard Henry (later Sir E.R. Henry) appeared before the inquiry committee to explain the system published in his recent book ”Classification and Uses of Finger Prints.” [16] The committee recommended adoption of fingerprinting as a replacement for the relatively inaccurate Bertillon system of anthropometric measurement, which only partially relied on fingerprints for identification. The Henry System of Classification was used by many european polices.

In 1905 U.S. Army begins using fingerprints. In 1918 Edmond Locard wrote that

if in a fingerprint comparison there are at least 12 points (Galton's Details) the two patterns come from the same finger (positive identification).
By 1946, the FBI had processed 100 million fingerprint cards in manually maintained files; and by 1971, 200 million cards.
From 2000 the automatic identification assisted by computer is introduced in many international polices; all US states and many european countries have their own AFIS databases, each with a subset of fingerprint records.

1.3.2 Fingerprint and the identification process

From the first applications for a forensic use to the last automatic systems (AFIS) the identification by fingerprints relies on pattern matching followed by the detection of certain ridge characteristics, also as known as Galton details or minutiae and the comparison of the relative positions of these minutiae points with a reference (or template) print. First of all during the comparison process, the fingerprint expert analyzes the whole pattern of the two fingerprints. In order to simplify this identification step it is constituted a classification system based on general ridge formations (i.e. the presence or the absence of circular pattern). The most famous and used system is the Henry Classification System [16] (the name from the father of the idea): both for the manual and the automatic identification process the classification of the general pattern is the starting point. In the Henry System there are three different main classification groups: Arch, Loop and Whorl fingerprint patterns.

Figure 1.2 shows the main four classification groups with some examples of fingerprint images.

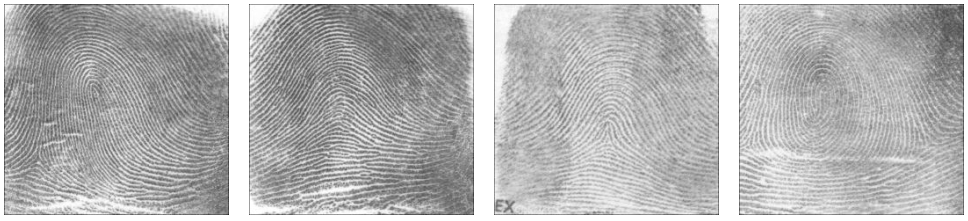


Figure 1.2: The main four classification groups for fingerprint.

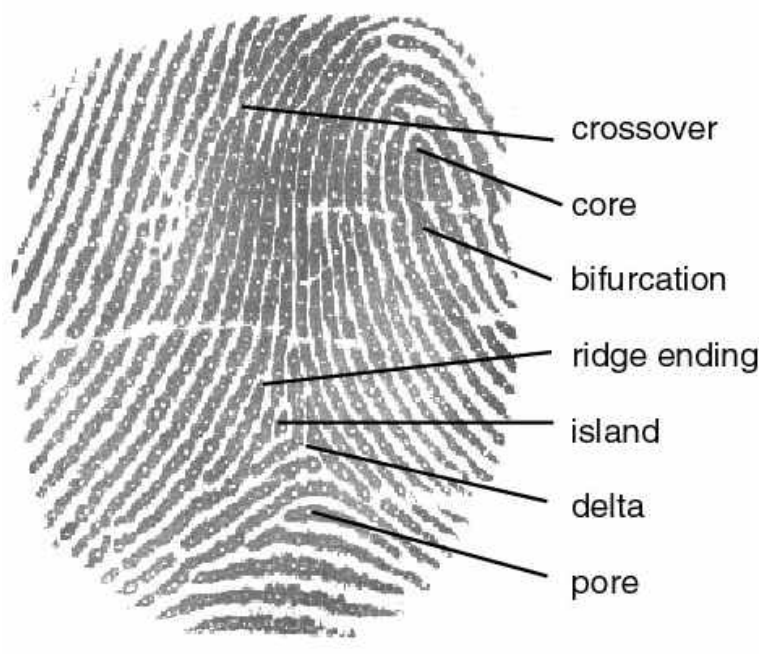


Figure 1.3: Representation of different minutiae points in a fingerprint pattern.

Figure 1.3 shows different types of minutiae points. Identification points consists of bifurcation, ending ridges dots and island and many other figures. These figures are formed by particular conformation of the ridges. A single fingerprint may have as many as 100 or more minutiae that can be used for identification purposes. In forensic field the fingerprint experts compare the two fingerprints in order to find a ”match”: the identification process consists in the analysis of all the matching Galton details. Basing on the law system of each country there are different regulations for the identification process. Generally we can distinguish two different approaches: a qualitative approach in which the expert gives an identity when, basing on his own experience in the field, finds a resemblance from a macroscopic to a microscopic view between the two fingerprints; a quantitative approach in which the law regulations dictates the minimum number of corresponding minutiae. In this last case the identity process ends when the counted corresponding minutiae exceeds the legal limit (in table 1.1 number standards for different country are presented).

1.3.3 Fingerprint in the automatic recognition systems

As we have seen before, fingerprints had a particular importance in a forensic laboratory for legal purpose. From this beginning application a remarkable number of industrial companies have proposed biometric system based on fingerprint data. First from academic groups and then from commercial purposes a lot of secure applications have proposed. Fingerprint biometric systems have occupied a wide range of applications both identification and verification types. There are a lot of examples of real applications in which fingerprint recognition is integrated. AFIS (Automated Fingerprint Identification System) is a system used for foren-

Country	Numeric Standard
Italy	16
Belgium	12
Austria	12
Cyprus	16
Denmark	10
France	12
Spain	10
Brazil	12
Colombia	10
South Africa	7

Table 1.1: Minimum number of correspondent minutiae for a legal identity

sic purpose, a fingerprint (generally found on a crime scene) is compared with a database of known prints. Nowadays many nations in the world have their own databases filled of millions of fingerprint. The large number of data recorded in the police servers involves an enormous computational burden during matching step. Therefore, AFIS systems are designed in order to optimize data storage and speed automatic computation. In this last years also civil AFIS are presented in the market of biometric system: for example the control for voter registration, driver licensing and public assistance. Concerning authentication biometric system, the typical use is access control. A system is integrated in the access of a real or virtual area with the aim of control access: fingerprint authentication system is integrated in some ATM (it is significant the South America market for fingerprint biometrics used to identify ATM customers), in the entrance of military or public

Biometric Identifier requirements	Biometric system requirements
Universality, distinctiveness, permanence, collectability, circumvention	Accuracy, availability, comfort, costs, circumvention

Table 1.2: Biometric identifier and system performance evaluations.

places (In Orlando, Disney World scans fingerprints of park visitors) or simply to authenticate in personal computer (from the first prototype by HP in 1998 to the more recent computer with swipe fingerprint sensor between the touch-pad buttons). Among the numerous type of biometric systems, fingerprint based ones have reached an high diffusion in world market. As we can see from the previous examples and from the market/economic implications (a detailed report is presented in figure 1.4) whilst a regular increase of biometric market is predicted for this decade, the major share of biometric technology is occupied by fingerprint systems.

1.4 Performance of a biometric system

In order to give an explanation of this large diffusion of fingerprint biometric system it is obligatory to make a preliminary remark about the performance evaluation of a biometric system. A complete characterization of a biometric system involves, first, a valuation of the biometric datum and then a valuation of the entire system. In table 1.2 two lists referred to these two performance sets are presented. A possible comparison of biometric identifier is reported in table 1.5.

A first consideration from this last table regards the fingerprint-based biometric systems: due to the well balanced evaluations of the esteem parameters this

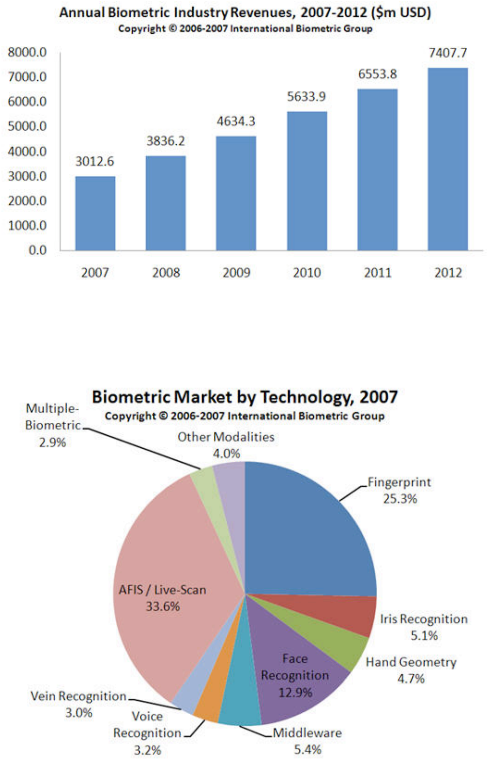


Figure 1.4: Composition of biometric market and revenues from 2007 to 2012 (From [17])

Biometric identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
DNA	H	H	H	L	H	L	L
Ear	M	M	H	M	M	H	M
Face	H	L	M	H	L	H	H
Facial thermogram	H	H	L	H	M	H	L
Fingerprint	M	H	H	M	H	M	M
Gait	M	L	L	H	L	H	M
Hand geometry	M	M	M	H	M	M	M
Hand vein	M	M	M	M	M	M	L
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Odor	H	H	H	L	L	M	L
Retina	H	H	M	L	H	L	L
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

Figure 1.5: Comparison of biometrics from [20]. H for High, M for Medium and L for Low. The comparison evaluations are subjective perception of the authors.

type of biometrics has a wide diffusion among the others. Further, a fingerprint biometric system responds to all the characteristics of a good automatic system. Good accuracy (as testified by all the last International Fingerprint Verification Competitions [19]), quite inexpensive (with about 100 euros it is possible to buy a fingerprint scanner with the matching software) and good public acceptability. Another issue that can be drawn from these two tables 1.2-1.5 concerns *circumvention* parameter: the security threats involve both biometric identifiers (i.e. the possibility to fake a biometric data) and systems (i.e. an intrusion attack against the entire system). The fusion of the security level of the identifier and the systems gives the global security of the entire biometric systems. This open the discussion about biometric security that is presented in details in the next chapters.

Chapter 2

Security and biometry

2.1 A preliminary overview

Security is a focal point in biometric application. Actually such technology is designed mainly to answer security and authentication tasks. This fact has given an high push to academic and industrial research in the study of biometric security. The concept of security for biometric systems has a wide range of meanings. This chapter is devoted to draw an exhaustive overview about all concerns this topic. Such technology interacts with ”personal” data which in some cases can hold important information about an individual, its health or simply about his/her presence in a place. For this reason ”privacy right” is joined to biometric systems and in particular to the storage and treatment of biometric information. Then the chapter shows the problem of circumventing and compromising such systems: all the possible fallacies of a real system are proposed.

2.2 Privacy and biometry

Privacy and biometry are always considered two connected arguments: first, because biometry treats about personal data, second, because biometry is related to access control, and so, control the human free movements, then because the acquisition of biometric data can be done in certain invasive modalities. In order to evaluate potential privacy risk in biometric systems, it is necessary to consider not only the biometric data but also the entire system. Therefore a lot of aspects that must be considered for judging privacy invasiveness, can be summarized with the following ”issues” :

- Are users aware of the system’s operation ?
- Is the system optional or mandatory ?
- Is the system used for identification or verification ?
- Is the system deployed for a fixed period of time ?
- Is the deployment public or private sector ?
- What is the context of the system ?
- Who owns the biometric information ?
- What type of biometric technology is being deployed ?
- Does the system utilize biometric templates, biometric images, or both ?

Are users aware of the system’s operation ? Deployments in which users are aware that biometric data is being collected and used, and acquisition devices

are visible, are less privacy-invasive than hidden deployments. User consent and awareness are principle keys for privacy-right. Hidden biometric systems are partially allowed only where a security risk is threatened (i.e. video-surveillance control in airport gates or in other public buildings).

Is the system optional or mandatory ? A biometric system in which enrollment is compulsory, such as a public sector program or one designed to control company's employees, shows a more direct relationship with privacy risks than an optional system. Different protections for mandatory and optional systems should be developed.

Is the system used for identification or verification ? A system capable of performing 1:N searches can be considered more susceptible to privacy-related abuse than a 1:1 system. A one-to-multiple biometric system would be necessary for use in any indiscriminate large-scale searches. Protections regarding 1:N usage may need to be more strict than more employed in one-to-one usage also because there is a major number of sensible informations. A typical applications of a 1:N biometric system is AFIS for forensic purposes.

Is the system deployed for a fixed period of time ? In deployments where such an option exists, the use of biometrics for an undefined duration has a negative impact on privacy than one deployed for a fixed time. This applies in particular to public surveillance deployments. When deployed for an indefinite duration, the risk of privacy violation increases.

Is the deployment public or private sector ? Government collection of biometric data without proper controls and restrictions is highly problematic. On the other hand, private sector companies may be more tempted to share or link personal data for marketing or profiling purposes. Suitable protections should be developed for

each type of environment.

What is the context of the system ? There are a lot of different conditions in the interaction between the system and the user. There are biometric controls that guarantee user security (i.e customer in commercial trading), others that guarantee the security of a population (i.e. the security control in a public place), others are employed in forensic applications or for prisoner identity (control the identity of a person for the security of others). All these applications have different conditions for storing data in a safety mode with or without explicit, informed permission of the individual.

Who owns the biometric information ? Some biometric systems, especially in authentication modality, offer the possibility to storing biometric data in a smartcard in possess of the user. In this case there is no privacy violation because each user has his own personal information. In some public sector uses it is not possible this: a central storage system that contains all the informations is connected with peripheral biometric terminals. This situation where storage unit and authentication one are physically separated has a different risk for the privacy violation.

What type of biometric technology is being deployed ? Behavioral biometrics are much less likely to be deployed in a privacy-invasive fashion, as technologies such as voice-scan and signature-scan can be easily changed by altering a signature or using a new pass phrase. Behavioral biometrics are very rarely used in 1:N applications, which are less privacy-sympathetic than 1:1. Physiological biometrics are much harder to mask or alter, and can be collected without user compliance.

Does the system utilize biometric templates, biometric images, or both ? Biometric systems in which identifiable biometric images or samples are retained are more likely to bear privacy risks than those which retain only templates. Biometric

images are generally identifiable, and can be associated with a specific individual based on visual inspection. Concerning fingerprint verification system, some recent works try to demonstrate how it is possible to reconstruct of a fingerprint image from some template minutiae point information.[25] As we can observe from all these previous privacy conditions, it is necessary to protect both the data from acquisition to the storage both the modality of acquisitions: the privacy right regards also the relation between the user and the biometric system. In table 2.1 the major biometric technologies are reported with their correspondent privacy risk.

In the last years the legal system of many countries in the world has put a particular attention on the problem of the privacy. The need of this legal formalization began from the conflict between privacy and security. In some countries (such as France) privacy is a constitutional right explicitly referred, in other countries without constitutional privacy protections a series of juridical initiatives have been proclaimed (i.e. in United Kingdom with the *Data Protection Act 1998*, in Australia with the *Privacy Act, 1988*). In Italy, after the *personal data protection code* in 2003 [22], it is noticeable to refer the recent attention of the ”Garante della Privacy” concerning the protection of biometric data in forensic and security application [23]. Currently, the Italian parliamentarian members are proposing an initiative about the institution of a DNA database for secure purpose.

2.3 System vulnerability

In the previous section we have dealt with the problem of privacy right and biometric data acquisition: we have seen the need of a protection of this personal data

Technology	**Privacy Aspects**	**Risk Ratings**
Fingerprint	Storage of images in public sector applications, use in forensic applications, strong identification capabilities	H
Face	Easily captured without consent or knowledge, large number of existing images can be used for comparison	H
Iris	Current technology requires high degree of user cooperation, very strong identification capabilities, development of technology may lead to covert acquisition capability, most iris templates can be compared against each other - no vendor heterogeneity	H
Retina	Requires high degree of user cooperation - image cannot be captured without consent, very strong identification capabilities	M
Voice	Not capable of identification usage, Can be captured without consent or knowledge	M
Signature	Signature images can be used to commit fraud	L
Keystroke	Can be captured without knowledge/consent	L
Hand	Physiological biometric, but not capable of identification, low cooperation of the user	L

Table 2.1: Principal biometric technologies and correspondent privacy aspects. The risk rating is by an evaluation of IBG for Bioprivacy Initiative [21]

during and after the acquisition process, in this section we cover all the intrinsic vulnerabilities of a biometric system.

As the diffusion of biometric systems becomes wider, interest of the information technology community is focusing on the methods of circumventing and compromising biometric systems. This care for the protection of biometric data comes from two evident points. First, the protection of biometric data means a protection of the person: a wider use of biometric recognition, in particular for forensic purposes, makes the biometric data very sensible with respect to privacy rights. The greater difficulties of designing a biometric system like AFIS concern security protection from external attacks. Secondly, biometric data are unchangeable for a person: the gravity of a biometric datum theft consists in the fact that the offended person ”lost” his/her identity forever. In order to face with this resounding question, it is necessary : (i) to prevent the biometric datum theft, (ii) to design secure biometric systems capable to detect a fraudulent attempt. Concerning item (ii), in this section, we focus on the main biometric system weakness. In figure 2.1 the principal vulnerability points are shown for a biometric system from the acquisition (at the scanner device) to data storage. In particular each arrow indicates the position of the vulnerability with the corresponding description.

1. *Denial of Service* - This attack consists in the turning off the system or in the hardware damaging. The use of adverse condition of employment in the system can suspend the correct functionality. The aim of these threats is to create a confusion and alarm situation.

2. *False Enrollment* - The user offers to the system a false identity. This is typical for passport frauds where by presenting a fake identity, the person can

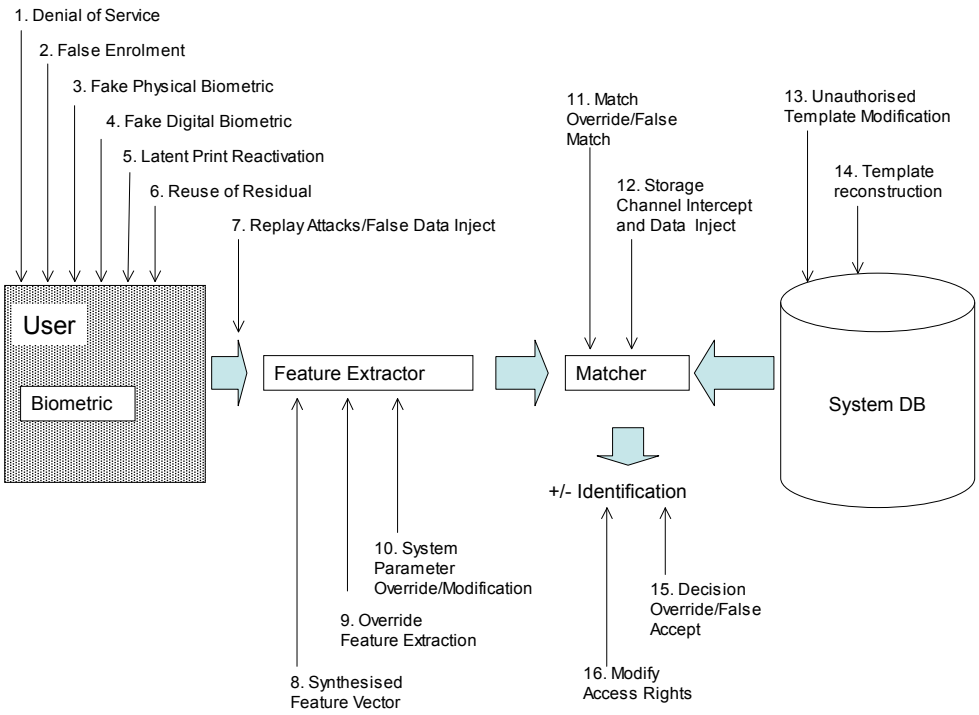


Figure 2.1: Biometric attacks and vulnerabilities.

be false registered. With the possession of a wrong identity, it is impossible to trace the cheat.

3. *Fake Physical Biometric* - The user submits a fake identity. This is the most studied vulnerability because with simple methods it is possible to reproduce artificially a fake biometric datum (fingerprint, face, iris, voice...). In this case the fake identity generally is a real identity of another person. In addition to fake artificial reproduction there is the (not negligible) possibility of a physical coercion: "Police in Malaysia are hunting for members of a violet gang who chopped off a car owner's finger to stole his vehicle protected by a fingerprint recognition system" (BBC News, 31 March 2005). This item represents the plot along which this Ph.D thesis develops.

4. *Fake Digital Biometric* - The fake information is submitted into the system directly in a digital type. This attempt requires a knowledge of the biometric architecture and a direct access to the system.

5. *Latent print reactivation* - Fingerprint/Palm acquisition requires that the user puts his finger on a surface and holds while the scanner records the morphology of the fingertip surface. The contact between the skin and the surface produces the transfer of a latent print from the sweat glands. The latent print left on the surface can be reactivated (made visible) through a range of techniques. When the biometric datum is visible can be recorded again by the system (for fingerprint scanner generally placing a plastic bag with water over the latent print).

6. *Reuse of residuals* - Some systems keep in a memory unit the last biometric datum. Accessing to this unit makes possible to repeat the last authentica-

tion procedure by submitting the last stored datum. Also this attack involves a deep knowledge of the system architecture.

7. *Replay Attack/false data inject* - After the first acquisition of the biometric device the information is passed to the next elaboration unit. This information chain can be altered with the intake of an altered data. The encryption by the input device of the information makes this attack more difficult.

8. *Synthesized feature vector* - This class of threats consists in the injection of fake information after the feature extraction block. Most of the biometric systems reduces all the biometric systems in a limited number of principal features (minutiae point for fingerprint, geometric measure for hand geometry and hear, a mono-dimensional signal for iris...). The attack inserts in the system a set of this type of features.

9. *Override feature extraction* - A typical example is the tampering of the feature extractor block. This alteration can be software or hardware based.

10. *System parameter override/modification* - The percentage of False Acceptance Rate (FAR) and the corresponding False Rejection Rate (FRR) determines the accuracy of a biometric system. In order to have an efficient system the optimal condition is to have a trade off among these parameters. The alteration of these values modifies both the accuracy and the security of the system: an increase of the FAR involves the increase of the impostors penetration rate.

11. *Match override/false match* - This is the tampering of the matching block output. The result of matching operation between user input and template information can be modified, overridden or ignored.

12. *Storage channel intercept and data inject* - The access to the storage mean involves a security and privacy violation. This threat consists or in the acquisition of a template datum for a later use or in the injection of a false template.

13. *Unauthorized template modification* - This attack hits the integrity of the template data management. The corruption of template information (for instance in the association between a user and his/her template) can subvert the identification or authentication process. In this class of attacks is also the physical corruption of template block included.

14. *Template reconstruction* - Generally the information in the storage unit is constituted by the extracted features from the biometric datum. Although this approach reduces the possibility of a fraudulent reuse of the encrypted datum, recently, for fingerprint systems, the possibility of reconstruct a complete fingerprint image only from the template minutiae points has been showed by [25]- [27].

15. *Decision Override/False accept* - This is a form of modification of the decision of the biometric system. In particular for authentication applications the biometric system controls a door for the access in a secure space. In this case the hacker tampers the control signal from the biometric system to the entrance allowing the access. This threat can involve a modification of physical connections.

16. *Modify access rights* - By obtaining system administrator privileges, a malicious user can modify the access rights of the registered users or other sensible operations of the entire system.

This detailed classification of all the possible threats in a biometric system has been compiled in the work [24]. The author distinguishes different vulnerabilities considering the modality and the location (in the system) of the attack. It is noticeable to consider how all these vulnerabilities have had an important contribution for the development of new sensing technologies and new biometric architectures. Next, three type of countermeasures are reported:

- *Data protection*: encryption of the data in the whole system, watermarking (any modification of the image can be detected), steganography (hiding template information in a cover image), application of a transformation to the template (or "cancelable biometrics").

- *Architectural solutions*: multiple biometrics (different biometric data), multimodal biometrics (different features for one biometric), liveness detection.

- *Sensing technologies*: touch-less (for fingerprint a 3D model of the finger is obtained), high resolution acquisition, multi-spectral.

It is important to remark that no systems can be completely secure and no single defensive mechanism comprehensively can protect the system. A part from this, the real esteem of the vulnerability of a biometric system involves also the risk assessment. This is the background about biometric security in which this thesis develops the "fake fingerprint" question: the next chapter describes in details the biometric systems vulnerability concerning on fake fingerprints, next, the thesis shows all the actual solutions developed in order to face this threat.

Chapter 3

Fingerprint reproduction

3.1 Fraudulent access

In the previous chapter all the threats for a biometric system have been presented: from biometric acquisition spoofing to data storage tampering. In this chapter we focus on the threat described at item 3 with the name of "Fake Physical Biometric": the attempt of authentication in a biometric system by using an artificial replica of the biometrics.

The following sections treat, after a previous overview of biometric trick access, the problem of fingerprint spoofing since the first attempt to the current research activity in the academic world. In the next chapter of this thesis the question of security is faced concerning the main countermeasures against fingerprint spoofing. Not only fingerprint but also a lot of biometric data can be spoofed. In 2002 Lisa Talheim in a magazine paper [37] suggested some test in order to fraud biometric devices.

Iris spoofing

The simplest spoofing method consists in getting a photo of the eye and reproduce a printed copy of the iris. Another solution is submitting directly the image of an iris by an LCD or a CRT monitor. One of the last attempt is the reproduction of the iris pattern on a contact lens applied on the surface of an eye.

Figure 3.1: Example of hand geometry spoofing from [29].

Hand Geometry spoofing

Hand geometry recognition is based on some geometrical measures of the hand: the scanner does not need to be presented with a 3D hand but only the side views are captured. The scanner records the hand profile and from this it computes the main measures. Features extracted from a presented hand shape are matched against stored genuine templates for verification check. In the work of H. Chen et al. [29] the authors have proposed two real implementations of making a fake hand. Both methods are used to fraud a real system based on hand geometry

recognition (HandKey II). The first method utilizes a fake hand made by plaster powder. After the creation of a mould, the space of the hand is filled with a mixer of plaster and water. The plaster hand is then used to spoof the hand geometry system. The second method consists in the creation of a silhouette of the hand from a captured images. This fake reproduction is made on a 2D paper card. It is demonstrated that the system is insensitive to the changes in the thickness of the hand. As showed in the paper the hand geometry recognition is a system vulnerable to spoof attacks.

Face spoofing

Although numerous face recognition methods have been presented, the question of spoofing face recognition systems is faced rarely. The most common faking way is to use a facial photograph of a registered user [37] [30]. The easy availability of humans face photos (download by internet, get a picture of a face with an hidden camera...) gets the spoofing attacks more achievable.

Others biometric data can be more or less easily spoofed: system based on voice recognition can be spoofed by a recorded voice, hand vein recognition systems can be fooled with a picture reproduction of the pattern.

All these threats are studied by research groups with the intention to test the security of different biometric systems. Whilst new spoofing attacks are discovered, corresponding new countermeasures are proposed in order to face these fallacies of the systems. In the field of spoofing attack a particular attention must be payed on fake fingerprint attacks. In the following section we redraw the history of fake fingers since the first attempt to the newest fake fingerprint dataset of different research groups.

3.2 The reproducibility of the fingerprint

If we want to understand the high interest on fake finger reproduction we have to consider the fundamental contribution of this type of biometric datum in the identification history. Fingerprint is and has been the most important mean in order to recognize unknown person, first for forensic purposes then in biometric applications. This crucial position of fingerprint in the identification process has increased the attention of deceitful intentions. In the next paragraphs we review all the attempts for reproducing fingerprints from the first trials to the last scientific works.

3.2.1 An overview of the artificial fingerprints

The first hints of fingerprint reproduction came from two different fictional works between the end of 19th century and the beginning of 20th century. In the novel "The adventure of the Norwood Builder" by Sir. A.C. Doyle [31] there is the attempt of forgery trials by the reproduction of a fingerprint made with a wax mould. Although this reference is a fantasy work there is, for the first time, the idea of fingerprint reproduction, the novel was presented on Strand Magazine in 1894. Later another detective novel [32] related about the recovery of a fingerprint and the doubts about its authenticity. Although the perception of copying fingerprints was present in the fantasy of some writers none has still consider this question as a real problem. The first recipe for fingerprint forgery came from Albert Wehde [33]. In the Twenties he was a photographer and an engraver, he spent a lot of his life to find a method to replicate a fingerprint: he left a fingerprint on a surface and after applying white powder to enhance the latent print he photographed it.

With the impression of the pattern he made a copper etching in order to create a 3D pattern of the negative. This copper was used to forge latent prints. He was the first man who proposed the copying of a fingerprint by photo-lithography. These attempts were only trails with no statistical nor scientific fundamental. In 1998 Wills and Lee proposed on Network Computing [34] the first work with a scientific value on spoofing biometric devices through fake fingers. The authors tested the security of six devices submitting fake silicon fingers: four of these six scanner were fooled by the attempts. Another method proposed by the authors consists in the reproduction of fake fingerprint from latent print: they used dry toner to enhance latent print, after the fingerprint was printed on a transparency. The thickness of the ink created was used to make the 3D pattern. In 2000 T. Putte and Keuning [35] demonstrated the possibility of easily fraud optical sensors with mean of silicon replicas of fingers. The experiment was conducted with six devices (optical and solid-state sensors), and all of them recognized fake fingers as live ones. For the first time the authors proposed two different methodologies for the creation of fake fingers, with and without cooperation of the user. Only in 2002 Matsumoto and others [36] undertook a milestone research in the field of fake fingerprint. The group led by Tsutomu Matsumoto at the Yokoama National University in Japan tested fingerprint system with silicone artificial finger. They verified that capacitive and some type of optical scanner reject artificial fingers because of the material chosen. In order to overcome this problem they made fake fingerprints with gelatin: the composition of gelatine (collage and water) allowed to obtain replicas similar to the human skin. This first experiment was conducted only with five subjects. All the systems considered (eleven scanners) falsely accepted the artificial fingerprints. They considered four different experiments in

which enrollment and verification steps were conducted with live and fake fingerprints. In particular with enrolled live fingerprints they tested that the systems accepted the artificial fingerprints more that 67 % of the time. In 2002 Liza Talheim et al. [37] extended the security test on others type of biometric systems (face and iris): they tried to spoof fingerprint scanner with alternative methods (i.e. breathing on the surface of the scanner, putting a water bag or dusting with powder to enhance the latent print). They used also silicone artificial fingerprints where the molds were made by heating wax. Optical and thermal scanners were fooled using this method. In 2002 [38] examined the security of a particular model of scanner with different methods of frauds. The method that gave better results was based on the use of gummy finger from a live finger mold (over 90 % of the trials).

A similar test [39] on a different device (Precise Biometrics 100 SC Scanner) was conducted in March 2003 by Stén, Kaseva and Virtanen. Best results were obtained with gelatin fake fingerprints (they showed that simply breathing on the scanner was not enough to fool the device). In August 2003 [40] two German hackers claimed to have developed a method based on the reproduction of latent print: Using graphite powder and tape to recover latent print, the fingerprint was photographed and then the image used to photo-etch a copper plate. This etch is then used as a mould for the silicone liquid. This was the first attempt for the creation of an high quality fake fingerprint from a latent print. In the same year, in October, Blommé et al. [41] proposed an evaluation of security of biometric devices against gelatine fingerprints. Once again the scanner were fooled by artificial fingers (results varied between users and scanners technologies, the acceptance rate was 25-50 % of the trials). In 2002, while several research groups

tested the security of biometric devices against fake fingerprint at the Biomedical Signal Analysis Laboratory at West Virginia University, USA, S. A. C. Schuckers with her group [42] developed new liveness detection algorithm based on the concept of fingerprint image processing. With this work the question passed from the study of the fallacy of biometric systems to the development of countermeasures against fake fingerprints. After that these works showed that it is possible to deceive a biometric system with fake fingerprints, in recent years the attention moved to the study of more efficient liveness detection methods. In the following Section, we describe the main reproduction technologies followed by different groups.

3.2.2 Reproduction technology

The reproduction technologies can be classified into two classes:

- *with cooperation*: (1) The user put his finger on a soft material (Play Doh, dental impression material, plaster...) - Figure 3.2. (2) The negative impression of the fingerprint is fixed on the surface - Figure 3.3. (3) A mould is formed. Silicone liquid or another similar material (wax, gelatine...) is poured in the mould. (4) When the liquid is hardened the stamp is formed - Figure 3.4.

- *without cooperation*: (1) A latent print left by an unintentional user is enhanced by a powder applied with a brush - Figure 3.5. (2) The fingerprint is photographed and then the image is printed in negative on a transparency - Figure 3.6. (3) The paper is placed over a printed circuit board (PCB) and then exposed to UV light - Figure 3.7. (4) When the photosensitive layer

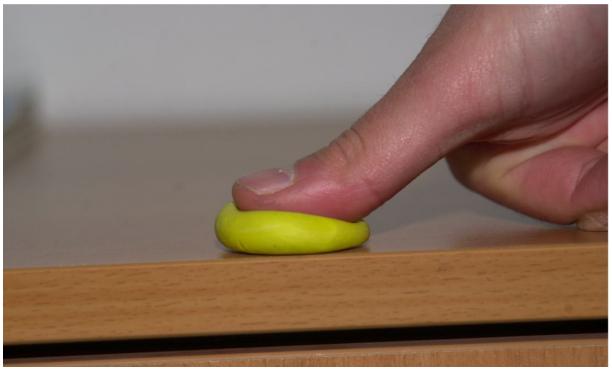


Figure 3.2:

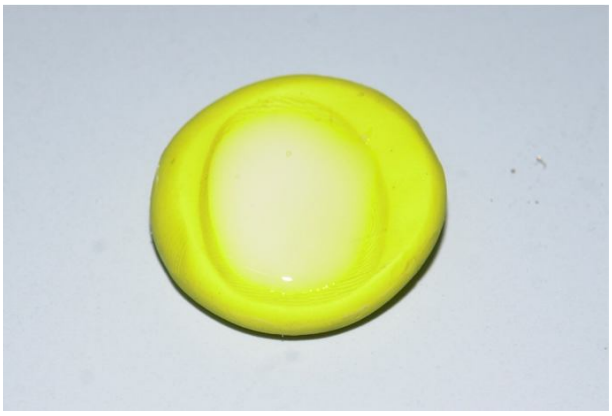


Figure 3.3:

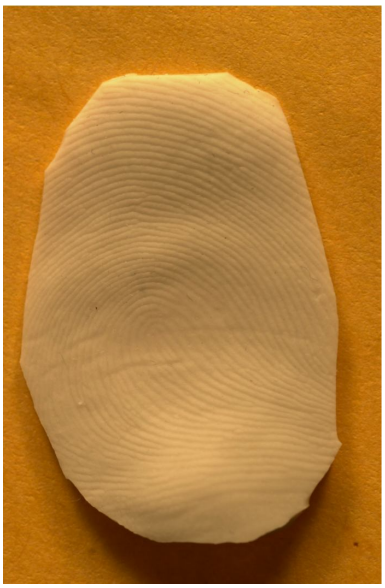


Figure 3.4:

of the board is developed the surface is etched in an acid solution - Figure 3.8. (5) The thickness of pattern in the copper is the mould for the stamp - Figure 3.9. (7) As for the cooperation method a liquid silicone (gelatine or wax) is dripped on the board - Figure 3.10.

Figure 3.5:

Figure 3.6:

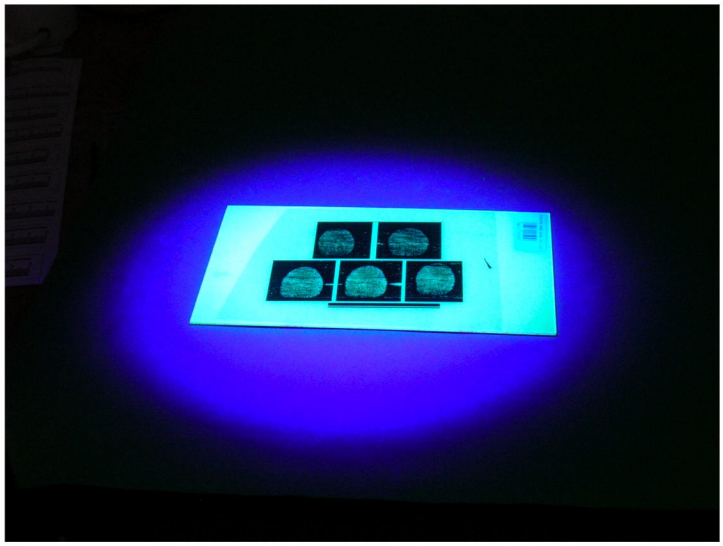


Figure 3.7:

Figure 3.8:

Figure 3.9:

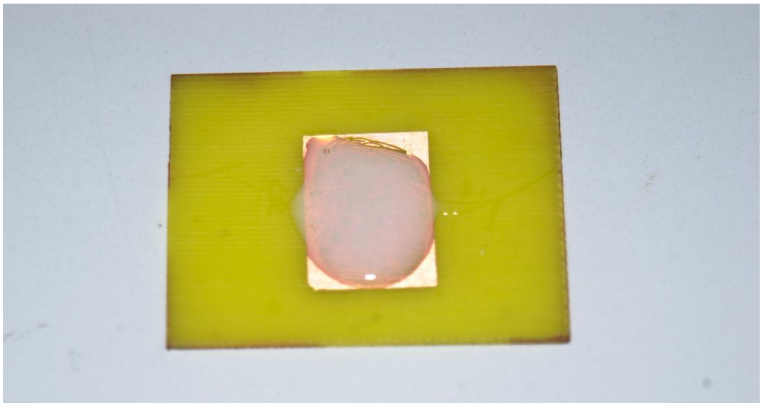


Figure 3.10:

Chapter 4

Methods for vitality detection

4.1 Introduction

In the previous chapter we have showed the possibility of deceiving fingerprint capture devices by submitting a ”fake” fingerprint made up of gelatine or other artificial materials. In particular we have seen the procedure for creating a replica of a fingerprint from a live finger (consensual method) or from a latent print (non-consensual method). In order to face with this threat, a biometric device must ”decide” if the finger on the acquisition sensors is alive or ”fake”. In other words, the recognition process must be upgraded with an added function for detecting the ”vitality” of the submitted biometric: after that the user presents his fingerprint, the system looks for some vitality hints and recognizes if it is ”fake” biometric. This procedure is called ”vitality detection”. In scientific literature several methods to detect the fingerprint vitality (or ”liveness”) have been proposed, and this research field is still very active. In the following sections we draw a survey of the main liveness detection methods proposed in the literature. We distinguish all

the methods, firstly, on the basis of liveness measures, then, on the basis of the dataset employed and their performances giving a comprehensive comparison of the results obtained.

4.2 The vitality detection in a biometric system

A possible taxonomy of fingerprint vitality detection methods is proposed in Figure 4.1 (for a reference correspondence see table 4.1). At first , existing approaches can be subdivided in ”hardware-based” and ”software-based”. The first ones try to detect the vitality of the fingertip put on the sensor by additional hardware able to measure physiological signs. These approaches are obviously expensive as they require additional hardware and can be strongly invasive: for example, measuring person's blood pressure is invasive as it can be used for other reasons that for simply detecting the vitality of his fingertip [52]. Moreover, in certain cases a clever imitator can circumvent these vitality detection methods. Therefore, making the image processing module more ”intelligent”, that is, making it able to detect if a fake finger has been submitted is an interesting alternative to the hardware-based approaches. Several approaches aimed to extract vitality features from the fingerprint images directly have been recently proposed [53]-[59]. The general rationale behind these approaches is that some peculiarities of ”live fingerprints” cannot be hold in artificial reproductions, and they can be detected by a more or less complex analysis of fingerprint images. The related vitality detection approaches can be named ”software-based”.

According to the taxonomy of Figure 4.1, the initial subdivision of the software-based approaches is based on the kind of features used. If the features extracted

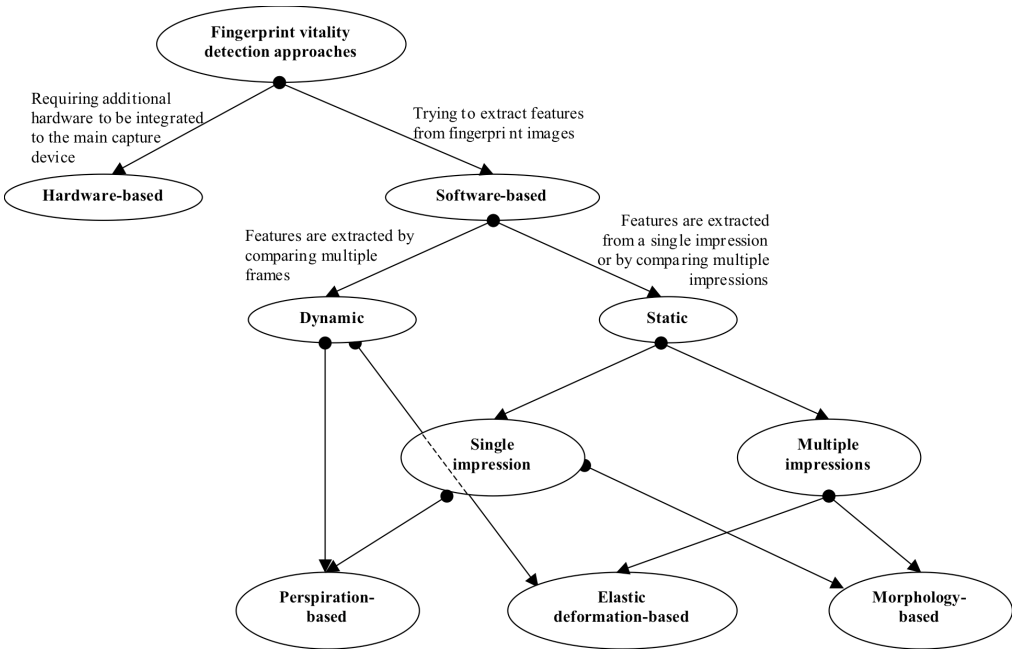


Figure 4.1: The proposed taxonomy of fingerprint vitality detection methods.

Liveness Detection Methods	**Reference Label**
Dynamic- Perspiration based	[53],[56],[58]
Dynamic- Elastic deformation based	[57]
Static- Single impression - Perspiration based	[53],[59]
Static- Single impression - Morphology based	[55]
Static- Multiple impression - Elastic deformation based	[54],[58]
Static- Multiple impression - Morphology based	[58]

Table 4.1: Fingerprint vitality detection and corresponding references.

derive from the analysis of multiple frames of the same fingerprint, captured while the subject puts his fingertip on the acquisition surface at certain time periods (e.g., at 0 sec and at 5 sec), the related methods are named ”dynamic” (as they use dynamic features) . On the other hand, if features are extracted from a single fingerprint impression or the comparison of different impressions, the methods are named ”static” (as they use static features). Referring to the leaves of the taxonomy in Figure 4.1, they describe software-based approaches as functions of the physical principle they exploit: the perspiration, the elastic distortion phenomena, and the intrinsic structure of fingerprints (morphological approaches). According to the proposed taxonomy, in the following sections, we review the vitality detection methods proposed in the scientific literature.

4.3 Hardware solutions

This classification includes all the additional devices integrated in biometric systems in which the liveness detection is carried out by an hardware device. Generally all these methods concern analysis on the fingertip: the device looks for specific physiological signs in the fingertip . A lot of US patent have been filed concerning liveness detection. Some functional principles that guarantees a liveness detection are reviewed in the following:

Optical property - A method proposed in 2005 by a biometric factory exploits a multispectral analysis of the fingertip skin: living human skin has certain unique optical characteristics due to its chemical and physiological composition which affects optical absorbance properties. The light source in the scanner is formed by LEDs of various wavelength. By collecting im-

ages generated from different illumination wavelengths passed into the skin, different tissue layer features may be measured and used to ensure that the material is living human skin.[45]

Pulse - A possible way for liveness detection is the analysis of the presence of pulse in the fingertip. This methods can be fooled by using a thin stamp applied under the fingertip. Another drawback of the measure is the long time for the acquisition (considering a mean pulse frequency of about 60 beats per minute, the user must hold the fingertip on the scanner for about five seconds). [46]

Pressure - A possible alternative for the previous methods consists in the blood pressure measure. [44]

Electrical Impedance - The electric impedance of human skin can range from kilo-Ohms to mega-Ohms depending on the wetness of the finger. Measuring these electrical properties of the fingertip surface, a fraudulent attack with an artificial finger can be detected. Also this technique can be fooled by wetting the artificial finger or using different materials of the reproduction (i.e. gelatine). [51]

Odor - A recent analysis of the odor has been proposed to liveness detection: an electrical nose is applied in the biometric device with the aim of recognize the typical material used to create fake fingers.[47]

Currently new technologies have been developed for liveness detection. The biometric system exploits some advanced acquisition devices in order to block fake replicas. Among these we can consider ”touchless sensor technology” [48]-[49]:

whole the surface of the fingertip is acquired by a 3D scanner. With such acquisition it is possible to detect an alteration of the anatomy of the fingertip. Another innovative solution concerns ”high resolution sensor technology” [50]. The device is upgraded with an high definition sensor: at high resolution it is possible to evaluate the conformation of sub-microscopic characteristics of the skin (poroscopy analysis). The absence of these particularity of the skin can be a valid help for recognizing artificial replicas.

Figure 4.2: Examples of touchless fingerprint scanner.

Moreover, there is a class of new approaches which has not a well defined position in the considered taxonomy: in the beginning multimodal and multibiometric acquisitions have been presented by scientific literature as new methods to improve recognition process and reduce recognition error (false acceptances or rejections). Submitting more than one biometric (i.e. fingerprint and face, or voice and face) can reduce false acceptance/rejection error rate and recognizing the user

can be easier than using mono-modal systems. Instead, the word ”multimodal” means that the user submits more times the same biometric (i.e. a fingerprint), and the system exploits different characteristics of this in order to univocally assign the identity. Currently these two different approaches are presented as possible vitality detection methods. Their classification is not easy: on one hand, these require additional hardware for the acquisition step, on the other hand, the measures fusion is based on software based algorithms.

4.4 Software solutions

4.4.1 Static systems: single impression algorithms

By following the path of the tree in Figure 4.1 from the static methods-junction, we first consider methods which exploit single impression. These can be classified into two further classes: perspiration and morphology based. About the former we have selected two main works as [59] and [53]. Both study the perspiration phenomenon with two transforms. In particular, Ref. [59] adopted wavelet space measure, Ref. [53] Fourier space measure.

Tan and Schuckers [59] showed how it is possible to clearly distinguish a live from a fake finger by wavelet transform. The rationale of this method is the analysis of the particular shape of the finger surface. In live fingers, in order to guarantee the physiological thermo-regulation, there are many little chinks named ”pores” scattered along the center of the ridges. Because of this characteristic the acquired image of a finger shows a non-regular shape of the ridges. Generally the path of the ridges is irregular and, if the resolution of the device is high enough, it is possible

to observe these pseudo-periodic conformations at the center of the ridges. With the fabrication step of an artificial finger it is possible to lose these micro-details and consequently the correspondent acquired image is more regular in the ridge shape. The authors propose to analyze this feature with a wavelet decomposition. In particular, the image is enhanced and converted into a mono-dimensional signal as the gray level profile extracted in correspondence of the center of the ridges. A wavelet decomposition of this signal is applied with a five-levels multiresolution scheme: The standard deviation, the mean value for each wavelet coefficient and from the original and the last approximation signals are computed. The obtained 14 parameters are considered as a feature-vector for the next classification stage. The concept of detecting liveness from the skin perspiration analysis of the pores has been already proposed in [53]. In particular, the authors uses one static feature, named SM, based on the Fast Fourier Transform of the fingerprint skeleton converted into a mono-dimensional signal. The rationale is that for a live finger it is possible to notice clearly the regular periodicity due to the pores on the ridges. On the contrary this regularity is not evident for spoof fingerprint signals. Another work is noticeable to mention. Unlike the previous works, this applies a liveness detection by studying the morphology of the fingerprint images. Thus, by referring to Figure 4.1, the branch ending to morphologic based method is related to the work by Moon et al. [55]. The study is based on a different method with a contrasting argument. Looking at the finger surface with an high resolution Digital Single Lens Reflex camera, they observe that the surface of a fake finger is much coarser then that of a live finger. The main characteristic of this work is that an high resolution sensor is necessary for successfully capturing this difference (1000 dpi, whilst current sensors exhibit 500 dpi on average). Moreover, this ap-

proach does not work with the entire image, too large because of its resolution, but with subsamples of a fixed size. For extracting this feature, the residual noise returned from a denoising-process applied to the original sub-images is considered. The standard deviation of this noise is then computed to highlight the difference between live and fake coarseness.

4.4.2 Static systems: multiple impression algorithms

Whilst the previous studies search a liveness indication from intrinsic properties of a single impression, there are other static features based on multiple impressions: in this case the liveness is derived from a comparison between a reference template image and the input image. While liveness signs are intrinsic properties of one fingerprint image (presence or absence of pores, residual noise) for the first, liveness detection is guaranteed by a comparison between one ”live” template with an unknown (live or fake ?) client for these new solutions. These methods are represented in Figure 4.1 with two branches starting from the ”Multi-impressions” node: one indicates methods based on elastic-deformation features, the other indicates morphologic features-based approaches.

Ref [54] falls within the first category. Given a genuine query-template pair of fingerprints, the entity of elastic distortion between the two sets of extracted minutiae is measured by a thin-plate spline model. The idea is that live and spoof fingerprints show different elasticity response repeating the acquisitions.

The experimental investigation in [58] considers both the elastic-deformation based method and the morphology-based one. The elastic deformation is evaluated by computing the averaged sum of all the distances among the matched minutiae of input and template fingerprints. The different elastic response of a live finger or

an artificial stamp is linked with the spread of this mean value.
The other static multi-impression measure is based on morphologic investigation. The feature that exploits ridge width (Ref. [58]) is based on the idea that during the creation of fingerprint replica, there is an unavoidable modification of the thickness of the ridges: first when the user put his finger on the cast material, next when the stamp is created with liquid silicone.
As we can observe all these measures (elasticity, morphological features) are user-dependent, and for this, it is need a multi-impression analysis.

4.4.3 Dynamic systems

Dynamic methods for vitality detection relies on the analysis of different image frames acquired during an interval while the user put his finger on the scanner. As shown in Figure 4.1, existing dynamic methods can be based on the perspiration phenomenon or on the elastic response of the skin.

While in [53] the periodicity of pores along the ridges is employed through a static measure to detect liveness of a fingerprint, in the same work the presence of pores is exploited by considering their physiologic property: the pores scattered on the fingertip surface are the source of the perspiration process. When the finger is in contact with the surface of the scanner, the skin gets wetter because of an increase of sweat amount. This physiological phenomenon can be recorded by acquiring sequential frames during a fixed interval of few seconds. The variation of the wetness of the fingertip skin reflects on a variation of the gray-level profile of the acquired images. In order to evaluate this feature, the fingerprint skeleton of the image at 0 and 5 seconds is converted into a couple of mono-dimensional signals ($C1$, $C2$). Several statistical measures are proposed on the basis of the

obtained signals. In particular [53], $DM1$ (Total swing ratio), $DM2$ (Min/Max growth ratio), $DM3$ (Last-First fingerprint signal difference mean), $DM4$ (Percentage change of standard deviation).

Ref. [56] can be considered as a prosecution of this first work, it draws up a more complete vitality analysis on different technology of fingerprint scanner and introduces some modifications to the original method. The dynamic of the device can produce a saturated signal for excessive amount of wetness, in such situation the feature $DM2$ lost its original efficacy. In order to avoid this drawback two new features named $DM5$ (Dry saturation percentage change) and $DM6$ (Wet saturation percentage change) are elaborated. With a selection of these measures, a liveness detection on an extended database is applied in [58].

A different approach of liveness detection based on elastic deformation is recently proposed by Antonelli et al. [57] : each user submitting his fingerprint rotates it during acquisition, thus producing a voluntary deformation of the fingertip surface on the scanner. The system acquires consecutive frames at high frame rate ($\geq$ 20 fps) during the rotation of the fingertip. It has been tested that live and fake data, due to the different composition of the skin and artificial materials, give different elastic response to that deformation. For each user the system compiles a ”deformation vector” from the dynamic measure. The vitality detection degree is estimated by comparing a client acquisition with the template ones. Since this method involves multiple frames of the same fingertip, each one representing a different impression, this new method can be classified in both static and dynamic methods.

4.4.4 Summing up

As we have seen from these last paragraphs, a wide range of measures both software-based and hardware-based are proposed in literature. Some of these involve deep modifications to the entire acquisition stage of the biometric: hardware based approaches request the complete replacement of the scanner interface while for some software based approaches (i.e. work by Antonelli et al. [57]) a new acquisition protocol is need to be implemented. The methods based only on image processing involve a lesser degree of modifications. The integration facility of a liveness method is important also for a major acceptability of the system to the user. From this point of view, measures based only on image processing of the fingerprint acquired by the scanner can be considered better than the others. For these approaches the liveness analysis is hidden to the end user. A comprehensive evaluation can be given only after the analysis of the performances of each methods. In the next sections we compare the entire testing protocol followed by all these software based approaches.

4.5 An overview of the dataset

In order to guarantee a complete review of previous works in this section we analyze: (i) the different materials employed for fake stamps and the methods used for creating them; (ii) the characteristics of the data sets used for the vitality detection experiments. Table 4.2 deals with Item (i) for the methods we reviewed in the previous Section. Item (i) is important because the response of a certain fingerprint scanner varies with the material adopted (e.g., gelatine or silicon). Secondly, the intrinsic quality of the stamp depends on the material for the cast and the method

followed for its creation. With regard to the mould materials, all those employed are able to deceive an optical sensor, as pointed out in [36]. In particular silicone or latex materials are more suitable than gelatine one in order to make a large set of stamps: gelatine moulds have a shorter life and must be employed at once after the creation. On the other hand, using silicone material is not effective for capacitive sensors: the water percentage in gelatine stamps gives an electrical property more similar to the skin. The fundamental property of these materials is the reproduction capability: for example, for silicone material the parameter "shore" indicates the hardness of the sample. We have to consider that it is need an high degree of softness for reproducing papillary details (less than 1mm). In Table 4.2 it is worth noting that all the approaches at the state-of-the-art used the consensual method for creating the stamp. This method exploits the subject cooperation whilst other approaches, e.g., the ones that produce a fake stamp from latent fingerprints, are more complex and requires more expert knowledge [36]. Moreover, the quality of stamps is intrinsically lower than that obtained with the consensual method. The consensual method is used for obtaining high quality stamps, in order to create a severe performance test for vitality detection. It is, in fact, easy to see that fraudulent attacks using high quality stamps are much more difficult to detect, whilst attacks with low quality stamps can be, in many cases, detected without using a vitality detection module (the fake impression is rejected as an impostor impression).

It should be noted that several variables are involved in the fraudulent access process, in particular: (1) the initial pressure of the subject on the cast; (2) the mould material dripped over the cast; (3) the contact of the stamp on the acquisition surface. These variables concur to alter the shape of the reproduced finger-

Ref.	**Scanner**	**Cast Material**	**Mould material**
[53]	Capacitive	Rubber	Play-Doh
[54]	Not specified	Gum	Gelatine
[55]	Digital cam.	Not specified	Gelatine, Plastic clav.
[56]	Optical, Electro-optical, Capacitive	Dental impression	Play-Doh
[57]	Optical	Not specified	Silicone, Gelatine, Latex
[58]	Optical	Plasticine	Silicone
[59]	Optical	Not specified	Play-Doh

Table 4.2: Software-based methods for fingerprint vitality detection and materials and methods used for stamp fabrication. All the acquisitions have been collected with consensual methods.

Ref.	**No. fakes**	**No. impressions**	**No. frames**	**Correspondence with clients ?**
[53]	18	1	2	NO
[54]	32	10	0	YES
[55]	24	1	0	NO
[56]	12	5	20	NO
[57]	33	1	2	NO
[58]	28	2	2	YES
[59]	80	1	0	NO

Table 4.3: Some key characteristics of the data set used for vitality detection experiments in previous works.

print and, in some cases, these alterations strongly impact on the final quality of the obtained image. Figure 4.3 shows some examples of fake fingerprint images where it can be easily observed the different visual quality. It is worth noting that no previous work has devoted much attention to this issue.

The second item we raised in this Section concerns the characteristics of the data set used for the vitality detection experiments. Table 4.3 points out the most important characteristics of the data sets used in previous works. The second column reports the number of different fake fingerprints (subjects), the third one the number of impressions for each fingerprint, the fourth one the number of image frames acquired. The fifth column points out if the subjects used for producing stamps are the same used as clients, namely, if the data set contains both fake and live fingerprint images for each individual.

Information reported in Table 4.3 is useful to analyze: (1) the sample size of

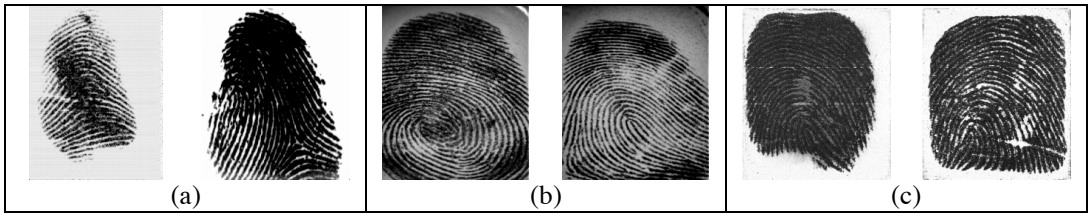


Figure 4.3: Examples of fake fingerprint images from Ref. [53] (a), Ref. [58] (b), Ref. [55] (c).

data sets for fake detection rate evaluation; (2) the protocol adopted in experiments.

With regard to item (1), it is worth noting that it requires several resources in terms of volunteers, time, and personnel devoted to stamp fabrication. In particular, volunteers must be trained to appropriately press their finger on the mould material, and a visual analysis of the stamp is necessary in order to obtain good quality images. Another important aspect is the ”reproducibility degree” of certain fingerprint: some particular fingerprint patterns with thin ridge or with the presence of micro-details are not suitable for the reproduction. Also for this, in order to produce an acceptable stamp, many trials are require. Since the solidification of the mould material can require several hours, this impacts on the number of fake stamps produced per time unit. As a consequence, reported experimental results can be affected by the small sample size of the used data set. This could cause a not reliable estimation of the detection performance.

The differences about the above item (2), i.e., the differences of the characteristics of the data sets, are pointed out by the fifth column of Table 4.3. The term ”correspondence with client” means that for each fake image, there is the correspondent

live image. This impacts on the experimental protocol used and the final goal of the experimentation. In particular, works for which this correspondence is absent are aimed to point out that the proposed feature(s) can allow to distinguish a fake image from an alive one only. Accordingly, they do not require the presence of related clients. On the other hand, they do not allow evaluating the penetration rate of the stamps in a verification system, that is, to assess the rate of fake fingerprints which would be accepted as live fingerprints.

As we can see, the architecture of each dataset depends on the finality of each related works: i.e. a correspondence between live and fake fingerprints is not need where the liveness detection is based on an absolute measure. In these cases a set of fake fingerprint images is compared with a set of images from live client. For these works liveness is not an user-dependent measure but an absolute property of the images. Other works find liveness signs as an user-dependent property: (Table 4.3, third and sixth rows), a certain number of live and fake fingerprint frames/impressions is captured from the same subject. This is due to the characteristic of the measure, which requires the comparison of the input impression with the related template client (e.g. elastic distortion or morphological measures [54],[58] which require an additional minutiae extraction step), and also to the possibility of evaluating the relationship between fake detection rate and verification performance. In this case the protocol adopted is a little more complex, because the fake detection features can be extracted only by the comparison phase. For example, the protocol adopted in [58] is made up of the following steps: (i) an impression has been considered as the template of the fingerprint stored in the system database. Generally this impression is chosen from live dataset. From these images it is extracted a template liveness measure and the related minutiae

set. (ii) From a second impression (as the image provided by system during access attempt) it is extracted a client liveness measure and the minutiae set. (iii) A matching comparison between the two set of minutiae is computed to identify a genuine attempt and so, only for a positive match (the client is the same with the registered user), a liveness analysis is applied.

4.6 Vitality detection performances

Table 4.4 reports a preliminary comparison of previous works in terms of overall miss-detection (classification) rate, that is, the average between the rate of ”live” fingerprints wrongly classified as fake ones and viceversa. Due to several problems, as the differences in terms of sensors used, data set size, protocol, and classifiers, it is difficult to fairly compare these values. As an example, the work by Antonelli et al. [57] uses a threshold-based classifier based on the mono-dimensional distribution of live and fake classes. This distribution has been computed by the Euclidean distance between template and input distortion codes. The threshold has been tuned on the ”equal error rate” value. This value is obviously different from the overall error rate usually considered for evaluating the performance of vitality detection systems. Moreover, the strong variations in error rates even when using similar approaches (e.g. see [54] and [58] , or [53] and [56]) suggest that a common experimental protocol is necessary in order to avoid the difficulty in interpreting reported results. Finally, an average error rate of 3-5 % even in small data sets makes these systems quite unacceptable for a real integration in current fingerprint verification systems, due to their impact on the false rejection rates (i.e. wrongly rejected clients) which could increase. For example, the best fingerprint

Ref.	**Classification method**	**Error rate**
[53]	Back-propagation neural network	0%
[54]	Support Vector Machine	18%
[55]	Threshold	0%
[56]	Neural Network, Threshold, Linear Discriminant Analysis	6% (capacitive sensor) 3% (electro-optical sensor) 2% (optical sensor)
[57]	Threshold	5% (equal error rate)
[58]	k-NN Classifier	6%
[59]	Classification Tree	5% (capacitive sensor), 13% (optical sensor)

Table 4.4: Vitality detection performance reported in previous works.

verification system at the 2004 edition of Fingerprint Verification Competition exhibited a 2 % equal error rate on average [65].

4.7 Concluding remarks

From the survey of current works on liveness detection we can notice the early state of the results. In particular, due to the many difficulties of collecting a wide and a statistical valid dataset, all the approaches are tested on an insignificant number of images and this makes more difficult the interpretation of the results. In order to generalize a performance analysis of liveness detection methods, a more general common protocol is need : International Biometric Group, (an interna-

tional organization of biometric industries that provides a wide range of services to government and private sector clients), has drawn a project ”Spoof 2007” [66] with the purpose of creating a global network about liveness detection for biometric systems (both for fingerprint and iris technologies). The importance of this work is to have defined a clear protocol in order to examine biometric spoofing. The entire project is divided in two main sections: the first focuses the efforts toward ”system resistance”, measuring the ability of a system to resist spoofing attacks; the second is the ”spoofing effectiveness” measuring the ability of a spoof technology to conduct a spoof attack on a biometric system. The fundamental step of this project is the collection of a spoof library of different (wide range of materials and reproduction procedures) spoof sources. The analysis is addressed also to verification systems: it is analyzed spoof attacks both for enrollment and authentication steps, defining a series of parameters for evaluating spoofing penetration rate (Spoof Acceptance Rate, Spoof Enrollment Count etc.) This work represents the last important contribution of the state of the art concerning liveness detection: it defines the limit of the research until now, and draws a clear protocol for future approaches. Our contribution has to be put into this context: from our first work [58] and during the whole period of Doctoral studies our intention has been, on one hand, the continuous collection of images from live and fake finger in order to create a wide dataset on which basing our experimentations, on the other hand, the development of new and more efficient methods of liveness detection. In the next chapter, after the description of our last ”spoof” dataset, we draw a first approach based on the fusion of the main typologies of liveness features. Basing on the measure of the state-of-the-art we study the effect of the fusion of these in order to improve the accuracy of detect spoofing attempts.

Chapter 5

Experimental investigation of liveness detection methods

5.1 Introduction

In the previous chapter we have proposed a classification of the main methods adopted in literature concerning liveness detection. We have underlined how software-based approach represents a more acceptable solution: vitality detection is provided by extracting some features directly from the fingerprint image. From the taxonomy showed in the previous chapter we have seen how many types of approaches have been developed exploiting different characteristics of the human physiology or some intrinsic features of fingerprint images. At present, it is difficult to establish if a feature shows a detection capability better than another. We believe that this is mainly due to the fact that performances of different features have been assessed and compared with different acquisition sensors, and using small data sets which could have obscured the relative merits of the features, due

to the small sample-size issues [58]-[55]-[64]. The aim of this experimentation is to uniformly compare the main features : each of this is applied on the same image dataset and the results are elaborated with the same classification tool. On the other hand, we demonstrate that using more than one feature could improve the detection rate when a data set large enough is available. In our first paper [58] we have started this investigation, the work presented in this Ph.D thesis can be considered as a follow up of that preliminary work. In this chapter we focus on the so-called dynamic and static features (from Figure 4.1), the first sections provide a deeper description of these two types of measure recalling the concept of ”frames” and ”impressions” based acquisition. Following, we show the importance of the fusion of these two types of measure in order to improve Live/fake classification rate. To one section is dedicated the description of our reference dataset collected at Department of Electrical and Electronic Engineering (University of Cagliari). The importance of this new mean is given by its sample numerosity and its completeness (it is drawn for both dynamic and static measure), thus allowing to draw more reliable conclusions on tested features. We also propose novel static and dynamic features which can further improve the vitality detection performance. This comparison is also aimed to identify the best feature, or the best feature subset, for fingerprint vitality detection.

5.2 Dynamic and static features

The categorization we used in this chapter is the one proposed in the taxonomy previously showed, and based on the concept of ”frames” and ”impression” of a fingerprint. Frames are intended to be images captured by holding the fingertip on

the scanner surface without moving it. Position of fingertip does not change during acquisition. On the other hand, impressions are intended to be images captured even at different periods of time but fingerprint can be moved during acquisition. The extraction of dynamic features requires a time dependent analysis of fingerprint images. Basically, a multi-frame acquisition is performed while the user holds his finger on the sensor surface. The algorithm based on dynamic features receives as input the extracted frames of each finger and gives a vitality response by comparing these time series images (usually only two frames are compared). All these features are aimed to characterize and analyse the skin perspiration process during the acquisition stage. Static features instead give a spoofing warning by considering how multiple impressions of the same fingerprint differ: this category of features includes deformation and statistic analysis. This approach based on static features studies the variability of the fingerprint images during different acquisition processes. Figure 5.1 exemplifies the basic operation mechanisms behind these two vitality measures: dynamic features check vitality properties from multiple frames extracted from one acquisition; instead static features are computed from multiple acquisitions (i.e., impressions) of the same fingerprint.

Table 5.1 shows the features investigated in this experimentation. The first column indicates the label we adopt to indicate the feature, the second column gives a short description of the feature, the third column provides the reference papers in which the feature has been originally proposed (the label used in those papers to indicate the feature is also reported). The following Sections describe these features in detail.

Label	Short description	Reference
DF1	Mean value difference on the skeleton	DM3[53]-[56] DF1[58]
DF2	Dry saturation fraction	DM5[56] DF2[58]
DF3	Wet saturation fraction	DM6[56] DF3[58]
DF4	Mean value difference on the image	DF4[58]
DF5	L1-distance of the histogram	DF5[58]
SF1	Elastic deformation	$G(P)$[54] SF2[58]
SF2	Mean intra-distance value	SF1[58]
SF3	grey level - mean value	This experimentation
SF4	grey level standard deviation	This experimentation

Table 5.1: List of vitality features investigated and correspondent bibliographic references. The letter D indicates a dynamic feature, while the letter S a static feature.

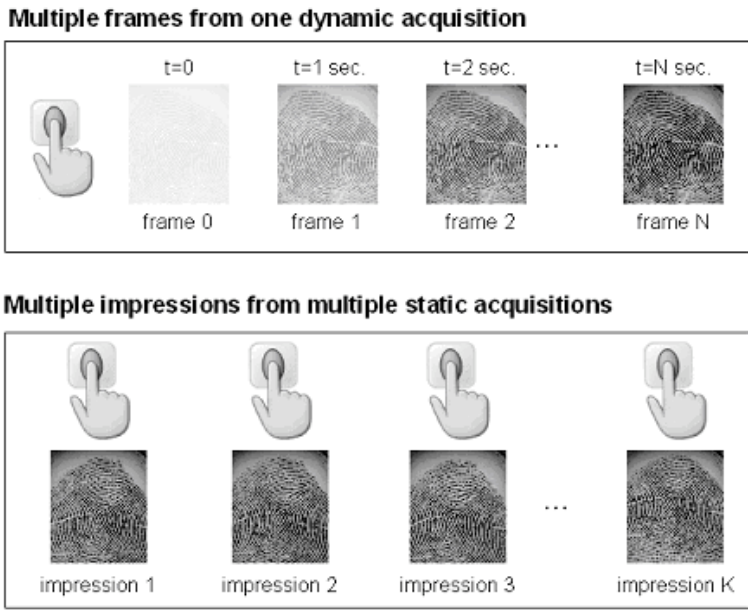


Figure 5.1: Multiple frame and multiple impression acquisitions used for static and dynamic feature extraction.

5.2.1 Dynamic features

The perspiration is a unique physiologic feature of the skin: the evaporation from the human body through the skin pores guarantees a correct thermal-regulation. In particular, the entire surface of the finger is characterized by the presence of a uniform distribution of pores. While the finger is in contact with the surface of a fingerprint-scanner this phenomenon can be observed with a slight change of the acquired images [53]. Due to the perspiration and the contact of the finger with the surface of the scanner the skin gets wetter and consequently the acquired images get perceptively darker (see also Figure 5.1). This physiological phenomenon is used as a vitality measure of the fingertip on the scanner, because it is generally not exhibited by a fingerprint stamp, due to the perspiration phenomenon absence. While the user keeps his finger on the scanner two images are captured with a

time gap of about 5 seconds. On the basis of this couple of images a set of vitality measures based on the differences extracted from the sequence is computed. The above differences are computed using only grey level values along the ridges path, and using these main processing steps:

- Acquisition of two frames of the same fingerprint temporally separated from 5 seconds;
- Binarization and thinning of the images;
- Creation of two mono-dimensional vectors $C1$ and $C2$ containing the grey level values of the extracted skeletons of the two frames;
- Processing of the differences of the two signals characterized with the above $C1$ and $C2$ vectors.

The fingerprint vitality degree is estimated from the differences computed. As pointed out in [53] these measures strongly depend on the acquisition stage. In particular, the output dynamic of the device strongly impacts on their reliability. Moreover, the perspiration phenomenon is not evident at the same degree in all persons (e.g. subjects with dry or moist fingers). In our case, the dynamic measures fitting the characteristic of the adopted optical sensor were (Table 5.1): the time difference of the mean grey level of the skeleton ($DF1$), the dry saturation percentage change ($DF2$), and the wet saturation percentage change ($DF3$). On the basis of the analysis of the perspiration phenomenon, we proposed and implemented two new dynamic measures computed on the entire image [58]: the time difference of the mean grey level ($DF4$) and the $L1$-distance of the histograms of two frames of the fingerprint ($DF5$).

5.2.2 Static features

The static features are the measures computed by using multiple impressions of the same fingerprint. The user repeats the acquisition of his fingerprint by removing and applying in sequence the finger on the scanner. In particular, a static feature is computed as the difference between a certain measure extracted from an input impression (to be assigned to an identity) and the one extracted from a template impression which is known to be from a live finger. It is worth noting that it is more difficult to find vitality discriminant properties among two impressions than among two frames. Many factors can alter a static measure: for example a different pressure of the finger on the scanner surface can modify the captured area of the fingerprint or the brightness profile of the image. The pressure can also modify the distribution on the finger surface of the elastic deformation. A first kind of static features is based on the elastic deformation of the skin. In particular, these features are based on the variation of the position of the minutiae set extracted from the image. Chen and Jain [54] showed how different distortion levels can partially be linked with the fingerprint aliveness. The rationale behind these approaches is the following. When a finger presses on a surface, the 3D flow of papillary ridges on the skin is leaved as a stamp on the surface as a 2D pattern. If the finger is on a scanner surface this 2D pattern is recorded as an image. The passage from 3D to 2D flow involves an elastic deformation depending, e.g., on the softness of the fingertip, the pressure of the contact, the orientation of the finger on the surface. For each finger there is a unique elastic response that can return a vitality measure when compared with a plastic fake stamp. In this work, we adopted the elastic distortion model proposed in [63] . We firstly extracted the set of minutiae from the two fingerprint impressions. By the so-called

String matching algorithm we detected the set of correspondent minutiae. [**?**] In this way we obtained two sets of ordered minutiae for two different impressions of the same fingerprint. Given $M_c = (m_{c1}, ..., m_{ck})$ and $M_t = (m_{t1}, ...m_{tk})$ the two minutiae sets for the comparison we first compute the Thin Plate Splines-model (TPS) by which we obtain the complete correspondence of the two set of minutiae.

$$F(M_c) = M_t \tag{5.1}$$

According to the TPS model, given the set of minutiae M_c - M_t, the function that forces the set M_c to a complete correspondence with the M_t set is described by the following TPS formula for each point:

$$m_t = F(m_c) = c + Am_c + W^T s(m_c) \tag{5.2}$$

where c is a 2 x 1 translation vector, A is the 2 x 2 affine matrix, and the third addend is related to the warping contribution: W is the (k x 2) matrix coefficient and the term $s()$ is the distance function $s(m_c) = [\sigma(m_{c1} - m_{t1}), \sigma(m_{c2} - m_{t2}), ...\sigma(m_{ck} - m_{tk})]$ with the basis function $\sigma(u) = ||u||^2 log(||u||)$, $\sigma(u) = 0$ for $||u|| = 0$. The correspondence of the two sets is generally obtained by a rigid and elastic distortion; the entity of the elastic deformation can be summarized in a real-value named bending energy. For a complete description of the Thin Plate Spline model the reader is referred to [63]. Accordingly, given the (k x k) matrix distance S, $S_{ij} = \sigma(m_{ci} - m_{cj})$, the expression of the minimized bending energy we used as a fingerprint vitality feature is as follows:

$$BE = trace(W^T SW) \tag{5.3}$$

Besides the bending energy ($SF1$), we adopted the difference among the mean values of the distances of the minutiae into a certain minutiae set ($SF2$). In other words, starting from one set of correspondent minutiae we have computed the mean of the sum of the distances with the other ones. By this parameter we collect the information about the spatial arrangement of a fixed minutiae set for each fingerprint image: once a template minutiae set has been established, by analysing the values spread for different impressions we can estimate the elasticity property of the fingerprint reproduction. More the object (fingerprint or fake stamp) is rigid, more the set of minutiae keeps a constant value of this parameter for each impression. Ideally a completely rigid stamp will produce always the same elastic distortion value.

Moreover, we introduce a novel kind of static features which are based on some statistical measures about the grey level of the image. These features are the mean value ($SF3$) and the standard deviation ($SF4$) of the grey level of the fingerprint image (Table 5.1). They can be considered as complementary of the dynamic ones, because they look for the same information, but in a multi-impressions context. Figure illustrates a case where dynamic features are not discriminant enough (see frames at the left hand) due to the poor contribution of the perspiration phenomenon of the subject. On the other hand, the correspondent statistical features succeed by comparing the second fake frame with the second template one, due to the appearances differences between live and fake impressions.

A different approach of liveness detection based on elastic deformation is recently proposed by Antonelli et al. [57]: each user submitting his fingerprint rotates it during acquisition, thus producing a voluntary deformation of the fingertip surface on the scanner. The system acquires consecutive frames during the rota-

tion of the fingertip. It has been tested that live and fake data, due to the different composition of the skin and artificial materials, give different elastic response to that deformation. For each user the system compiles a ”deformation vector” from the dynamic measure. The vitality detection degree is estimated by comparing a client acquisition with the template ones. Since this method involves multiple frames of the same fingertip, each one representing a different impression, this new method can be classified in both static and dynamic methods. The acquisition stage of this measure does not allow to combine this with the other features: this is not compatible neither with the dynamic measures (it is not possible to capture perspiration during the finger rotation), nor with the static features for which, as an example, the extraction of minutiae is required. However, since this method has shown to be promising, we are currently arranging an appropriate data set and experimental protocol to fairly compare it with other static and dynamic features, and this will be object of a future work.

5.3 The dataset

In order to investigate static and dynamic features, we collected a multiple-frames / multiple-impressions dataset. In particular, the steps involved in the creation of this set of images from the fabrication process to the acquisition are the followings.

Step 1 - Fabrication Process

Images were acquired from 82 different fingerprints from 50 people aged between 20 and 70 and the 72 fake stamps. The lack of symmetry is due to the impos-

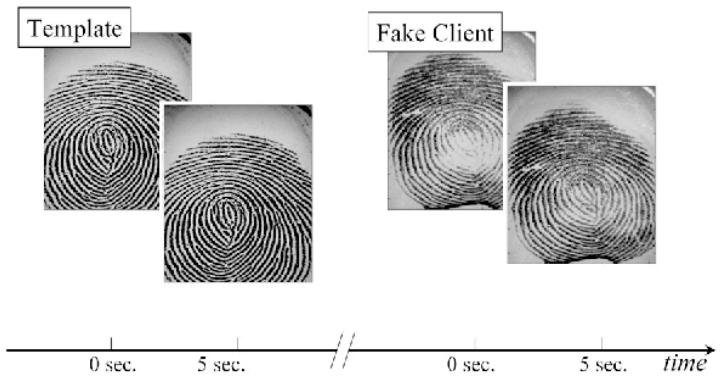


Figure 5.2: A case where dynamic features are not discriminant enough (see frames at the left hand) due to the poor contribution of the perspiration phenomenon of the subject. On the other hand, the correspondent statistical features succeed by comparing the second fake frame with the second template one, due to the appearances differences between live and fake impressions.

sibility to reproduce some fingers with the chosen material: fingertips with very thin ridges or with a damaged surface are very difficult to be reproduced and this does not allow to make a readable stamp. In the fabrication process of the fake finger we adopted the so-called consensual method, which is commonly followed for assessing the performance of fingerprint vitality detection features. [**?**] The basic steps of this process are: (1) the user put his finger on a plasticine-like material: the pattern of the fingerprint is negative reproduced in a mould; (2) the liquid silicon with a catalyst is dripped over the mould: the liquid covers the negative fingerprint; (3) after some hours the solidification of the rubber is completed and the cast can be removed from the mould; (4) the rest of the plasticine mould is cleaned off from the surface of the cast. This procedure was repeated for each different finger. In order to produce the replicas we used the following materials:

for the mould we employed a plasticine-like material that offers a good malleable property and a high stability in the time, for the cast we used a two-compound mixture of liquid silicone and a catalyst. The material of the cast is a high flexibility siliconic resin (SILGUM HF) with a very low linear shrinkage, less than 0.1 % (this is particular important for the reproduction of the details of a fingerprint with a dimension below a millimetre). The liquid catalyst (Stanne, Dibutyltin dilaurate) must be mixed with the silicone material with a percentage of 5%. Besides the high quality of replicas, the choice of the stamp material is suggested by the technology of the fingerprint scanner adopted: given the high opacity of the silicone material is particularly suitable for optical scanners that employ Frustrated Total Internal Reflection (FTIR). Another property of silicone material is the durability of its elasticity properties. On the basis of these considerations, we preferred the silicone material to another cheap opaque material like wood super glue: when the glue dried the stamp tends to crack. The obtained stamps are therefore characterised by high reproduction quality and particularly effective to deceive an optical sensor.

Step 2 - Acquisition Process

For the acquisition of the fingerprint images we used the Biometrika FX2000 optical sensor with an acquisition area of 25x13.2 mm^2. The size of images is 312x372 pixels. Each user was required to repeat for 20 times the acquisition of his fingerprint. For each acquisition a couple of time-frames at 0 and 5 seconds has been extracted. At the end of the acquisition process we have collected 3280 ”live” images (82 fingers x 20 acquisitions x 2 frames) and 2880 images from fake stamps (72 stamps x 20 acquisitions x 2 frames). Both high and low quality im-

ages have been included in the collection. The main features of our dataset w.r.t. data sets collected by other researchers are:

- A large sample size. As an example, the data set of Derakshani et al. [53] is comprised by 54 live and fake finger images, in Chen et al.[54] 640 live and fake images were collected. Our data set is comprised by 1640 live and 1440 fake finger images. By considering the second frame of each image, the overall dataset doubles its size. Another wide dataset proposed by Galbally [61] does not include multiple frames of the same fingerprint impression. Thus, it is not possible to use it as a data set for comparing static and dynamic features.

- In order to test both dynamic and static feature the dataset includes different impressions and different frames from each acquired finger/stamp.

- The dataset is comprised by high and low quality images. This wide range of quality values permits to testing the measures over different images and then to generalizing the results.

Step 3 Automatic Quality Assessment by NIST software

The quality of live fingerprint images is given by several factors: conformation of the live fingertip surface, quality of the sensor, etc. [67]. For artificial fingers, we have to consider also the fabrication quality of the stamp. A specific fingerprint image quality measure can be computed by the well known NIST quality checking algorithm [67]. Figure 5.3 shows the results of the NIST quality check on our data set. The algorithm assigned one of the five NIST quality levels to each fingerprint image. We can observe the wide spread of distribution from high quality level to the lowest.

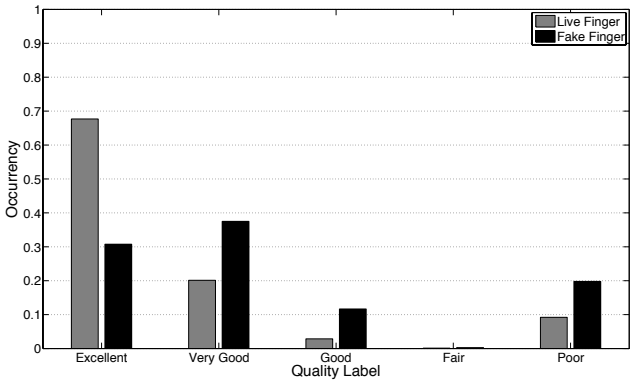


Figure 5.3: Quality classification of the images of our dataset. The five quality levels have been assigned by the NIST software Quality classification of the images of our dataset. The five quality levels have been assigned by the NIST software.

5.4 Experimental result

5.4.1 Experimental protocol

In order to extract static and dynamic features from fingerprint images, we adopted the following protocol.

- One live fingerprint impression for each client has been used as template image.
- Both for static and dynamic measure we have extracted a difference measure coming from template image and the related client. Where the measure does not need a specific couple of images (as for elastic deformation) an arithmetic difference has been computed from the two separated measures applied to the template and the client images.

- Dynamic Measures: we have computed the five dynamic measures ($DF1..DF5$) for the extracted vectors $C1$ (at 0 sec.) and $C2$ (at 5 sec.) from each couples of frames. The difference between the value from template couple and client one have been computed.

- Static Measures: measures from $SF2$ to $SF4$ have been computed separately from each template and client image. As the bending energy concerns, the elastic measure has been applied to the couple template-client images.

- Each difference feature has been normalized as follows:

$$f_i^{(n)} = \frac{f_i - \mu_i}{\sigma_i} \tag{5.4}$$

  Where $f_i^{(n)}$ is the i-th normalised feature ($i = 1, ..., 9$), μ_i and σ_i are the mean and the standard deviation of f_i over all available patterns.

Thus, we obtained 1558 feature vectors comprised by nine static and dynamic measures from live images, 1440 feature vectors from fake images.

In our work, we did not include the method by Antonelli et al. based on the "distortion-code" [57]. In fact, it is not possible to extract distortion-code because the investigated system used multiple frames and impressions pointed out in Figure 5.1. Static and dynamic features are compared fairly, because they are extracted in the same acquisition session in which user releases two frames of the same impression. The Antonelli et al.'s method needs an additional acquisition step, separated from that for other static and dynamic features, because, for example, it is not possible to capture perspiration measures during distortion-code acquisition. Accordingly, comparison of distortion-code performance and other

features could not be considered fair. Currently, we are arranging an appropriate protocol to fairly compare static and dynamic features with Antonelli et al.'s method, and this will be object of a future work.

5.4.2 Feature analysis

Table 5.2 reports the correlation coefficient of the investigated features on the whole data set. It is easy to note that all the considered features are lowly correlated, on average. However, there are some small differences. As an example, $DF1$ and $DF4$ exhibit a similar behavior in general, but their correlation difference with $DF5$ allows to hypothesise their combination could improve performance (correlation difference of $DF1$, $DF5$ and of $DF4$, $DF5$ is more relevant than that with other features). Among the static features, $SF1$ exhibits the lowest average correlation coefficient. In general, Table 5.2 confirms the results reported in [58], where the same sensor and material have been used for testing, but in this case the statistical significance of results is greatest due to the larger size of the data set used.

Figure 5.4 reports the range of values of each feature, and the degree of statistical separation between live and fake classes estimated by the so-called class separation statistic CSS [62], which is computed as follow:

$$CSS_i = \int |p(f_i|FAKE) - p(f_i|LIVE)|df_i \tag{5.5}$$

Where CSS_i is the class-separation statistic value estimated for the i-th feature, $p(f_i|FAKE)$ and $p(f_i|LIVE)$ are the distribution of the i-th feature given the fake and live classes, respectively. We estimated these distributions by the nor-

malized histograms method, also adopted in [**?**]. Thirty equally spaced intervals were used for each feature. With regard to the state-of-the-art perspiration-based features ($DF1, DF2, DF3$), we can notice a similar behavior. All these measures are overlapped and also the differences between mean values are strongly slight. This behaviour is observable also with the new dynamic measure $DF4$ while $DF5$ shows a lower overlap between fake and live values. Both $DF1$ and $DF5$ have the same C.S.S. test value but the first have a worst difference among live and fake mean values. Among static features, while $SF1$ and $SF2$ show a behaviour similar to the dynamic ones, both $SF3$ and $SF4$ have the best separation class separation values. The difference with the results showed in Parthasaradhi *et al.* [56] are probably due to factors as the small sample size issue affecting their dataset, or the dynamic difference of the optical sensors used: in this case, reported results contributes to point out the sensitivity of the perspiration-based measures which have to be carefully selected in dependence of the used capture device.

In order to provide further evidences, we report in Figure 5.5 the accuracy of individual features using the nearest neighbour classifier and the leave-one-out method for assessing the accuracy. Unfortunately, it is not possible to compare our results with that in [54],[53],[56] because no details on the best features have been reported in those papers. However, it is possible to compare some results with those reported in [58]. In general, we notice that the worst features are those with lowest class-separation statistic values ($DF2$, $DF3$, $SF1$,$SF2$). Both relative accuracy among features agreed with [58], but overall performance is notably different. These differences can be explained by considering that a small sample size issue probably affected the dataset in [58], thus related results could have

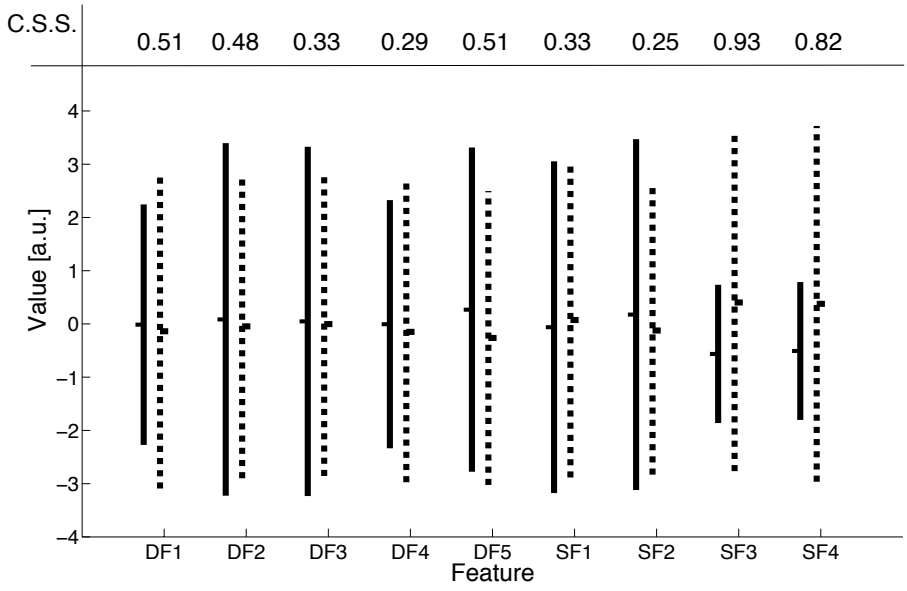


Figure 5.4: Range of values for all the features on live dataset (solid line) and on fake dataset (dashed line).

	$DF2$	$DF3$	$DF4$	$DF5$	$SF1$	$SF2$	$SF3$	$SF4$
$DF1$	0.02	-0.07	0.77	0.34	-0.10	-0.05	0.04	0.14
$DF2$	—	0.05	0.01	0.15	0.05	0.02	-0.07	-0.04
$DF3$	—	—	-0.09	0.01	0.05	0.01	0.01	-0.02
$DF4$	—	—	—	0.53	-0.10	-0.03	0.04	0.14
$DF5$	—	—	—	—	-0.03	0.07	-0.16	-0.08
$SF1$	—	—	—	—	—	0.03	0.08	0.02
$SF2$	—	—	—	—	—	—	-0.14	-0.12
$SF3$	—	—	—	—	—	—	—	0.42

Table 5.2: Correlation coefficient of static and dynamic features.

been over estimated [64].

Tables 5.3-5.4 report the percentage accuracy of best group of static and dynamic features. Groups have been selected by an exhaustive search over all possible subsets of adopted features. Each row of Tables 5.3-5.4 shows the best subset of features. It is possible to see that static and dynamic features exhibit the same performance accuracy when used together (Tables 5.3-5.4, last rows). However, it is reasonable to argue that they are able to recognize different subsets of the data set, that is, they could exhibit a certain degree of complementarity, which could be also suggested by their low average correlation coefficient shown in Table 5.2 (even if low correlation does not necessarily implies high complementarity).

Accordingly, we investigated the best subsets of features when using both static and dynamic ones and showed the related accuracy in Figure 6. Even in this case, an exhaustive search over all possible features subsets have been performed. It is easy to see that the best result is achieved when using two static features

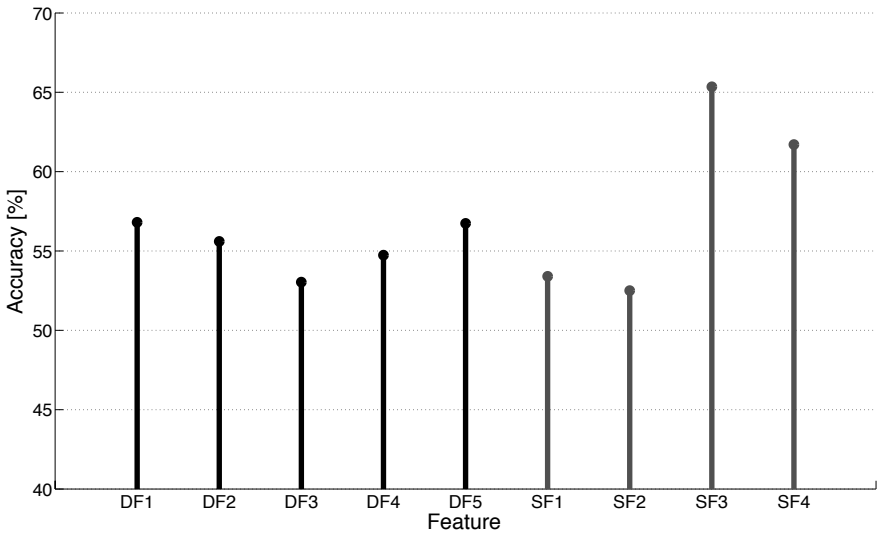


Figure 5.5: Accuracy percentage for each feature (black -dynamic features, grey - static features).

($SF3$, $SF4$) and all dynamic ones. A sharp performance improvement has been obtained. Generally we can observe a strong improvement with the use of multiple features (Figures 5.5-5.6). Two observations can be also drawn from Figure 5.6: (i) it is very difficult to exploit the elastic deformation differences between fake and live images (its contribute is negligible) this could be due to the different distortion features of our stamps with respect to those of the gummy replicas by Chen and Jain [54]; (ii) perspiration-based features, which exhibit a high accuracy variation used alone [58]-[56] increase the performance notably when used together. This means that they are so complementary that image characteristics missed by a feature can be captured by another one.

It can be noted that in Figure 5.6, the curse of dimensionality effect (the performance of the system drops once a certain number of features is reached) cannot

be observed. This is possible but not very common in feature selection problems. As previously pointed out, we performed an exhaustive search over all possible features subsets. Therefore, the effect of the curse of dimensionality[64] could be reduced. Other reasons can be referred (and worthy of investigations) to the representativeness of the data set (about 3000 samples covering possible fake and live fingerprint variations), the number of features not so large (less than 10), the small number of classes (2) and also to the fact that we adopted a leave-one-out classification strategy, which strongly decreased the spread off of training samples on the feature space because only one sample is always considered as test sample (as performing averaging on 3000-fold cross validation). From Figure 5.4, which shows the amount of overlapping between classes, it can be noticed the ranges of values for each feature are about the same, and cover uniformly the same amount of feature space. Worth noting, accuracy starts dropping when number of features is reaching the maximum (Figure 5.6): this can be explained with the addition of noisy features, maybe dependent on some outliers, which bring the sample to a region of features space not well covered by captured samples. In our opinion, these explanations does not explain the fact satisfactorily, and further investigations are needed to evaluate the impact of curse of dimensionality in this application.

Finally, we showed in Tables 5.5-5.6 the best features subsets when separately combining the state-of- the-art features and the ones we proposed in [58] and in this work. A better performance is obtained with the features we are proposing, thus confirming the suggestion reported in [56] about the need of novel measures exploiting the differences between live and fake fingerprint images. As shown in Figure 5.6 the classification performance can be further improved by using them together.

Accuracy [%]	**Subset**
56.80	$DF1$
60.74	$DF4$-$DF5$
65.38	$DF1$-$DF4$-$DF4$
67.88	$DF1$-$DF2$-$DF4$-$DF5$
71.71	$DF1$-$DF2$-$DF3$-$DF4$-$DF5$

Table 5.3: Percentage accuracy of dynamic features.

Accuracy [%]	**Subset**
65.34	$SF3$
73.42	$SF3$-$SF4$
73.18	$SF1$-$SF3$-$SF4$
72.11	$SF1$-$SF2$-$SF3$-$SF4$

Table 5.4: Percentage accuracy of static features.

Accuracy [%]	**Subset**
56.80	$DF1$
60.11	$DF1$-$DF2$
62.48	$DF1$-$DF2$-$DF3$
63.58	$DF1$-$DF2$-$DF3$-$SF1$

Table 5.5: Percentage accuracy for state-of-the-art features.

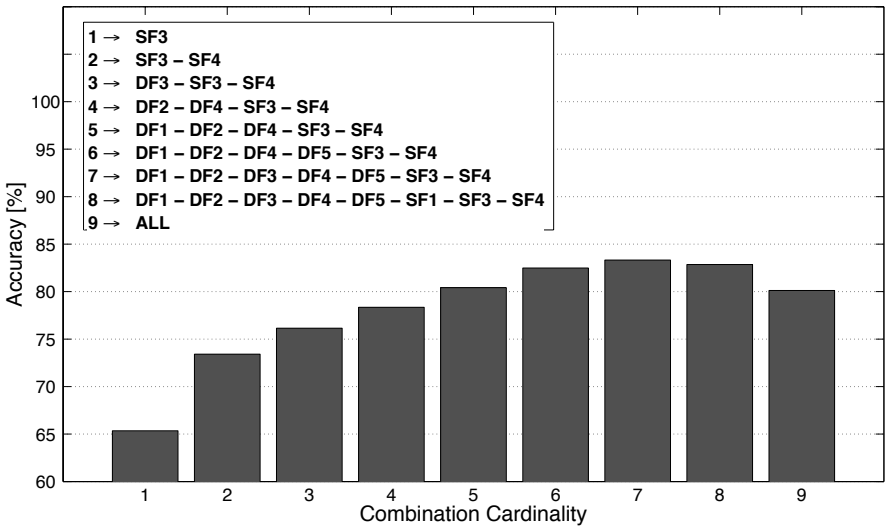


Figure 5.6: Overall percentage accuracy for feature subsets with cardinality from 1 to 9.

Accuracy [%]	**Subset**
65.34	$SF3$
73.42	$SF3$-$SF4$
74.25	$DF5$-$SF3$-$SF4$
77.75	$DF4$-$DF5$-$SF3$-$SF4$
75.35	$DF4$-$DF5$-$SF2$-$SF3$-$SF4$

Table 5.6: Percentage accuracy for proposed features.

Chapter 6

Advanced morphologic features for liveness detection

6.1 Introduction

From results presented in the previous chapter we can observe that: (i) the best features derive from measures disjointed from physiological or physics properties of the user but directly linked to properties of the image ($SF3$ and $SF4$ give higher accuracy values), (ii) the use of multiple features involves an evident increase of classification accuracy (from Figure 5.6 of about 30%). The first item can be explained from the irregular behavior of the physiological measures. Perspiration and elastic deformation of the skin are user-dependent features, not uniformly distributed in the population: some human diseases can alter the thermoregulation process, thus increasing or reducing the wetness of the skin. At the same time the hardness of the skin can influence clearly elastic properties of the tissue. For this reason it is not simple to find a correlation between such measures and liveness

detection ability. Item two is explained by the effect of the features fusion on the classification process: classification by means of different uncorrelated features can provide better results. In order to overcome the use of multiple features (thus simplifying the recognition process), we have addressed our research toward the investigation on features which have, alone, high fake-live discrimination power. In particular we have considered two morphologic measures. As described in the following sections, such measures exploit some intrinsic properties of the image: the first one, in the space domain, is based on the analysis of the differences of ridges width from a ”live” template and an unknown client; the second one, presented in [68], analyzes morphologic changes in the frequencies domain. Both of these measures are based on properties of the digital image (i.e. the high frequency in 2D-Fourier space) or on some changes involved by the fabrication of the stamps (i.e. the variation of ridge width from a live fingerprint to a fake one). By following the consideration at item (i), both of these features presented in this Ph.D thesis are user-independent.

6.2 Morphologic analysis in the space domain

6.2.1 Introduction

Figure 6.1 suggests the possibility of using the ridge width as vitality detection feature, as the ridges of a fake image are often very different from those of a live image. In our preliminary work [58] we have presented a liveness feature based on ridge width information: for each image it was computed a ridge width mean value. Although this static feature have the best accuracy among the other static

(a) (b)

Figure 6.1: Live fingerprint image (a) and correspondent, that is, related to the same finger of the same subject, fake fingerprint image (b).

ones, the classification capability of this is not enough for a real biometric systems. The averaging over the whole images reduce the classification accuracy of the feature. From this, the necessity of developing a more efficient liveness measure based on this morphologic property of the fingerprint pattern. The use of the ridge width as feature for fingerprint vitality detection comes from the analysis of the steps followed for the stamp fabrication. The phases of the ”consensual” method are summarised in the following: (1) The subject put his finger on a plasticine-like material for creating the mould consisting in the fingerprint negative. This step alters the ridge width due to the mould material hardness, the fingertip consistency, the pressure imposed.

(2) These moulds are filled with liquid silicon rubber to create wafer-thin silicon replicas. About one day is necessary for the solidification of the rubber. The ridge width can be altered by the viscosity and the elastic stability of the silicon.

(3) During the acquisition process, the stamp is pressed over the sensor surface. This further impacts on the ridge width of the obtained image. It is easy to show

that similar conditions hold even if fingerprints are reproduced by non-consensual methods, as the reproduction from latent fingerprints. In this case, the reproduction of the mask for the lithography (photography of the fingerprint, digital binarization of the image and printing on the transparency) can introduce a perceptible width bias.

6.2.2 Ridge width extraction

The global approach of ridge width estimation proposed in [58] showed a not adequate live-fake discrimination. In order to overcome this limit, we proposed a new approach based on a trade-off between a local measure (the punctual ridge width) and a global one: the averaging of the ridge width is applied over a tessellation of the entire image. The resulting vector is composed by the ordered mean ridge width values extracted from each sectors specified by the tessellation. Thus, the ordered vectors holds the spatial location of the computed main ridge width value. In order to apply this measure we consider a limited region centered at a reference point of the fingerprint image. In this work we used a circular area, but other shapes can be used as well (e.g. a square region). A tessellation similar to that proposed in [69] was adopted. For each sector of the tessellation, we computed a local average of the width ridges. An example of tessellation is given in Figure 6.2.

The main steps of our feature extraction algorithm are:

1 Choose a reference point in the image;

2 Consider a circular mask divided into N_s sectors;

Figure 6.2: Circular mask with 32 sectors.

3 Compute the width of the ridge along the fingerprint skeleton;

4 Extract a feature vector of N_s elements by averaging the values within the N_s sectors.

5 Parameters tuning.

Reference point. Almost all the procedures presented in the literature [20] for core detection are based on the analysis of the orientation field. For example, the Poincaré index method is one of the principal singularity extraction method. In this work we used a core detection method based on the identification of the discontinuities of the orientation field. The idea is that in correspondence of a singularity of a fingerprint (core, delta...) we have a maximum of the spatial variation of the orientation vectors. In order to return only one reference point we consid-

ered the center of mass of all revealed discontinuity points. The visual analysis of all the images of our home-made data set showed that this method guarantees a good localization accuracy of the reference point, in particular for images with close singularity points.

Creation of the mask. The next step of the procedure concerns the creation of the tessellation mask. A circular region is subdivided into a fixed number of sectors and centered at the reference point extracted. The size of the entire mask and of each sector is aimed to optimize the accuracy of the measure. The size of the tessellation must satisfy two requirements: firstly, a sector must be wide enough to enclose more than one ridges in order to return a more reasonable average width value; secondly, the number of sectors must be large enough to improve the accuracy in details of the tessellation: a large number of sectors allows obtaining a mask that faithfully reproduces the morphology of the image. In our experiment we have considered masks with 4 to 32 sectors.

Computation of the ridge width. The measure of ridge width and in general of the intra-distance between two consecutive ridges has had an importance in the sizing of denoising filter as shown by O'Gorman in [70] and by Yin at al. [71]. An initial morphologic algorithm is applied to the image in order to extract the skeleton from the ridge flow of the fingerprint (Figure 6.3a). The erosion reduce each ridge to a 1-pixel line. Then, from the original gray level image it is computed the flow directional field. For each point we obtain the mean value of the direction of the ridge flow $\theta(i, j)$. In order to avoid local discontinuities we have considered a grid quantization of 15x15 block size. Starting from each point of the skeleton we have traced the gray level profile along the orthogonal direction to the ridge flow.

As it is schematized in the third sketch of Figure 6.3, the signal extracted has

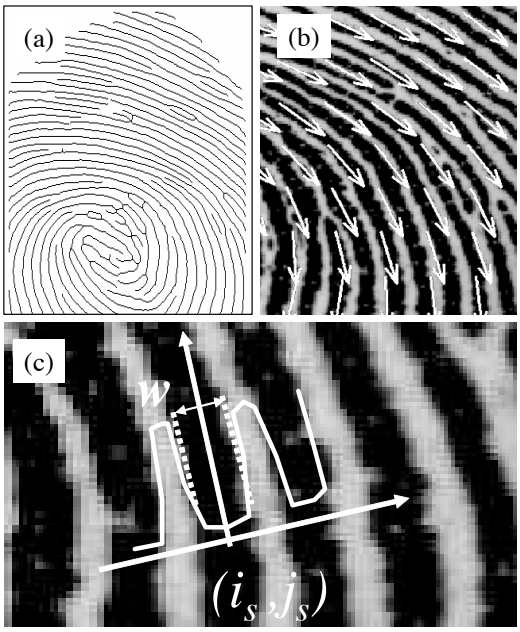


Figure 6.3: Main steps for the computation of the local ridge width: (a) extraction of the skeleton from the image, (b) orientation field, (c) estimation of the width for each point of the ridge.

lower (higher) values in correspondence of the ridge (valley). The ridge width has been estimated as the interval where the signal is under a fixed threshold.

Feature extraction. The local estimation of the ridge width have an high variability along the pattern of the fingerprint: inside the same pattern there are areas with different ridge thickness. Moreover, depending on the pressure of the fingertip on the sensor, we can observe a high variation of this local measure among different impressions of the same fingerprint. In order to consider a more effective width measure we averaged the values of the local quantity along each sector of the mask previously defined. The proposed feature vector contains the mean value of the ridge width for each sector of the circular area. Given a mask with N_s sectors, we can represent the K-th component of this feature vector $[W_1, ...W_{N_s}]$ with the following expression:

$$W_k = \langle w(i,j,\theta) \rangle \qquad i,j \in S_k \tag{6.1}$$

where S_K is one of the N_s sectors of the mask.

Parameters tuning. The last step of the feature extraction scheme is the sizing of the mask, in particular, the radius and the number of sectors. Two approaches are possible to this aim. First, considering that the average inter-ridge distance is approximately 10 pixels for a 500 dpi images (as it is reported in literature [69]), we can consider a radius and a number of sectors such that each sub-region includes a significant number of ridges: for instance, for a radius of 200 pixels and a mask with 16 sectors, the linear dimensions of the widest sectors is approximately of 100 pixels (along the radius direction) and about 80 pixels (along the circumference). This values are high enough in comparison with the main intra-ridge distance. The second approach is based on the estimation of

the two parameters through a validation set. The radius and the number of sectors maximize the classification accuracy on a fixed validation set. Obviously, samples in this set must be representative of the expected user population.

6.3 Morphologic analysis in the frequency domain

6.3.1 Preliminary remarks

In our opinion, no work at the state-of-the-art paid enough attention to the stamp characteristics achievable by using a certain material, and the quality of the stamps has been neglected so far. However, a simple visual analysis of high quality fingerprint images coming from stamps obtained with liquid silicon rubber (Figure 6.4) shows that there are some differences between live and fake fingerprint images. Such differences are mainly due to the stamp fabrication process which causes an alteration of the frequency high-level details between ridges and valleys, although the main properties of the fingerprint (minutiae location, ridge frequency) are unaltered. From this point of view, it is worth noting that although the Fourier transform is widely used in fingerprint image enhancement, classification, matching and quality evaluation [20], no work proposed features using this transform to distinguish live and fake fingerprints. The use of a study of ”live” and ”fake” fingerprint characteristics in the frequency domain is motivated by the above differences that cannot be captured by a human expert or state-of-the-art approaches for fingerprint vitality detection, unless using very high-definition electronic scanners [55]. Accordingly, in this chapter, we propose a novel feature based on the Fourier transform analysis for the fingerprint vitality detection when fake stamps

are made up of liquid silicon rubber. This approach is tested on a commonly used fingerprint image scanner. Reported experiments have been carried out on a home-made data set made up of 1440 fake and live fingerprint images acquired with an optical sensor. Results show that the proposed feature exhibits a high vitality detection accuracy.

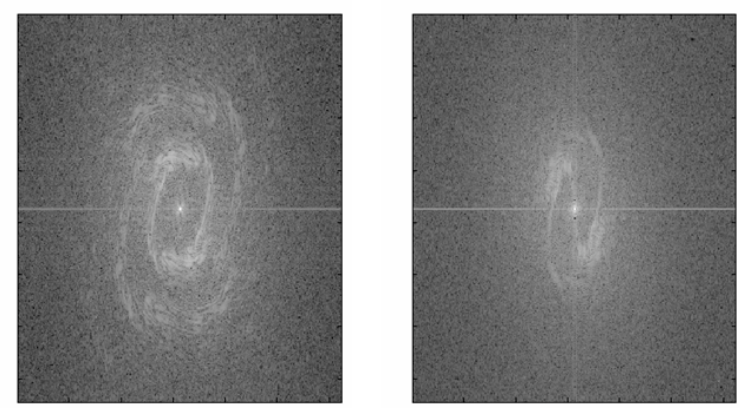
(a) (b) (c) (d)

Figure 6.4: Live and fake fingerprint images of the same finger (a-b). (c-d) Zoomed region from (a-b) in which it can be noted that high frequency details in the live image (c) are removed or strongly reduced in the fake image (d).

6.3.2 Fingerprint vitality detection in the frequency domain

In the commonly adopted process for generating fake stamps, namely, the so-called consensual method, the subject put his finger on a plasticine-like material. These moulds are then filled with liquid silicon rubber to create wafer-thin silicon replicas. About one day is necessary for the solidification of the rubber. It is easy to observe from Figure 6.4 that live and fake images exhibit some differences. Whilst the ridge-valley periodicity is not altered by the reproduction process, the main differences can be observed in the ridge profiles: some micro-characteristics, observable in Figure 6.4(c), and due to the roughness of the skin or to the ridge line discontinuity, are less defined in Figure 6.4(d), as very small cuts of ridge lines

increase their thickness (e.g. the transversal cut of Figure 6.4(c-d)). Consequently, high frequency details can be removed or strongly reduced. This can be analysed by computing the modulus of the related Fourier transform of the images, also called "power spectrum", as shown in Figure 6.5.



(a) (b)

Figure 6.5: Modula of the Fourier transform of Figures 6.4(a-b). Lighter pixels represent higher modula values.

It is evident that the live image exhibits more than one "mode" at a range of frequencies higher than that of the fake image. Therefore, analysing live and fake patterns in the frequency domain can be useful to extract novel features for vitality detection. Let $X(i,j)$ and $X_F(u,v)$ be the input fingerprint image and the related Fourier transform, respectively. Let E_S the energy of X computed for the frequencies of a given region S:

$$E_s = \int\int_S |X_F(u,v)|^2 dudv \tag{6.2}$$

The integration region S is given in terms of a circular region centred on the null frequencies along both axis. The radius of the region is indicated with R (spatial frequency units). In the following, we indicated with "High Frequency Energy" (HFE) the integral of $|X_F(u,v)|^2$ computed in the region out of S. This measure quantifies the amount of "residual" spectrum on the high frequencies. The rationale is that the HFE measure can characterise the information which distinguish fake and live fingerprints, as high frequency characteristics of fake fingerprints can be modified due to the reproduction process (Figure 6.4) and this is pointed out by their power spectrum (Figure 6.5).

6.4 The dataset

The performance test for both the morphologic measures is applied to a dataset created in the laboratory of the Electrical and Electronic Engineering Department of the University of Cagliari. The dataset is a wide collection of high quality images of fake fingerprint and the correspondent ones from live subjects. For the creation of the set we used the Biometrika FX2000 optical sensor. The acquired images have a dimension of 312x372 pixels. Images of the set have been acquired from 36 different fingers of a male population aged between 20 and 40. The fake fingers have been created with the consensual method . For each finger and its corresponding fake replica 20 different impressions have been acquired. A quality selection is applied in order to select only well defined fingerprint images. This last point is essential in order to correctly test both the ridge width and the power spectrum measures.

6.5 Performance assessment and results

6.5.1 In the space domain

In order to preliminarily assess the effectiveness of the proposed morphologic method, we carried out experiments using the nearest neighbour classifier and the leave-one-out method. Figure 6.6 shows the accuracy of the proposed vitality detection feature as function of the mask radius and the number of sectors (the number of sectors sets the size of the proposed feature vector). The radius ranged from $1/7$ and $4/7$ of the minimum image size. It is worth noting that the best results are obtained when the radius is around 200 pixels independently on the number of sectors. From the plot the best accuracy is obtained with a mask with 16 sectors, but it is worth noting that it is possible to achieve higher accuracy ($> 80\%$) not considering the 8 inner sectors of the mask. In this case we exclude from the measure the smallest sectors.

Two observations can be drawn:

- the mask size must be large enough to cover approximately all image but disregarding the noisiest portions of it (e.g. the ones near to the background, which are subjected to elastic distortion more than inner ones);

- the number of sectors must be such that the estimation of the average width in each of them is made on a significant portion of ridges.

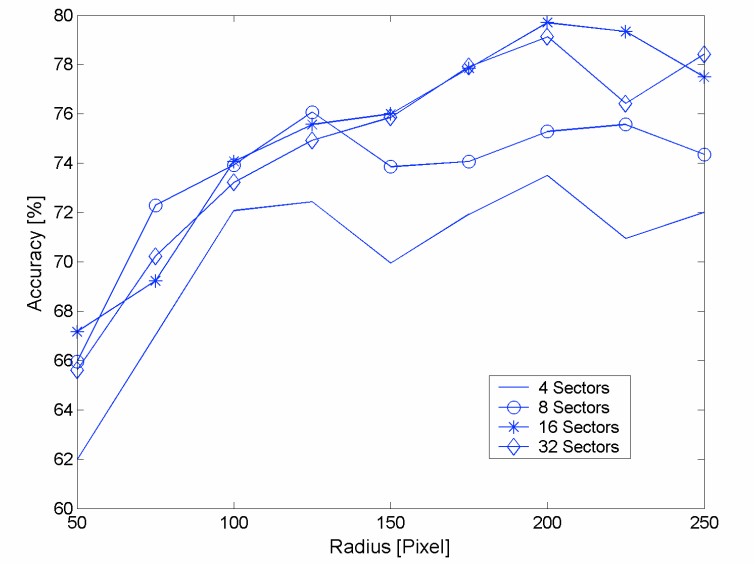


Figure 6.6: Accuracy of the nearest neighbour classifier using the leave-one-out method as function of the mask radius from 50 to 250 pixels, and the number of sectors (4, 8, 16 32).

6.5.2 In the frequency domain

Figure 6.7 shows the range of values of HFE measures, computed on the whole data set, for live and fake fingerprint images. The average, the minimum and the maximum values are reported for each value of R (the radius of the region), which ranges between 0 and $int[min(W, H)/2]$, where W and H are the image sizes. It is easy to see that the HFE range is such that the separation between fake and live fingerprint classes increases with high values of R. This can be explained by the fact that the "residual" details coming from the high frequencies are progressively filtered in the fake images, thus their power spectrum is significantly lower than that of live images.

Accordingly, we used the so-called Fisher distance (FD), which is a paramet-

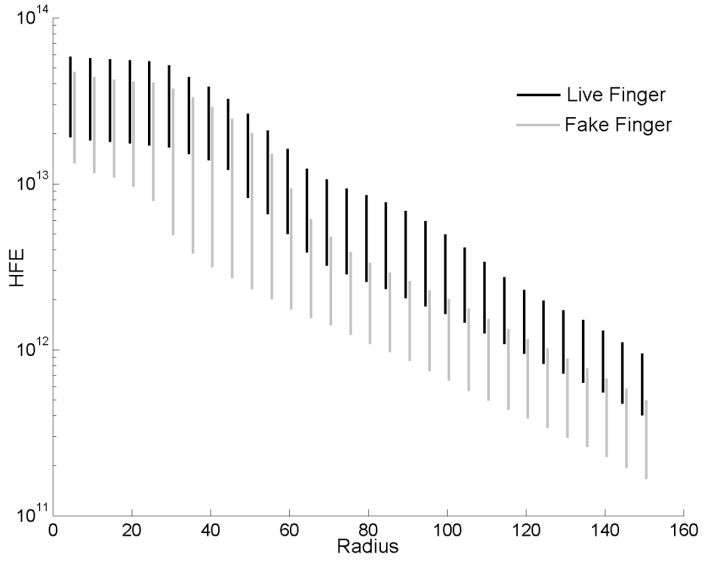


Figure 6.7: Range of values taken by HFE measures computed by varying the integration radius.

rical class separation statistic, for selecting the appropriate Radius value:

$$FD = \frac{(\mu_L - \mu_F)^2}{\sigma_L^2 + \sigma_F^2} \tag{6.3}$$

In eq. 6.3, μ_F, σ_F and μ_L, σ_L are the mean and the standard deviation of HFE measure for the fake and live patterns of the data set, respectively. We selected the value of R which maximises the above Fisher distance. Then, we adopted the threshold-based classification approach [56], [59]: if the HFE measure is more than a pre-defined threshold, the image is classified as a live fingerprint, otherwise it is classified as a fake fingerprint. In fact, the amount of residual energy for live fingerprints is higher than that of fake fingerprints (Figure 6.5). In order to assess the classification performance of the HFE measure, we applied the following experimental protocol: Subdivide the whole data set D in three partitions D_T, D_V, D_X. Estimate with D_T the R value for which the correspondent Fisher Distance is

maximum. Compute with D_V the threshold t for which the rate of images wrongly classified as "fake" fingerprints, is equal to the rate of images wrongly classified as "live" fingerprints. This error value is commonly called Equal Error Rate (EER). This threshold is computed by using the HFE measure computed as a function of R. Evaluate the classification error rate with D_X by computing the HFE as a function of R and using the above threshold t. The error rate has been evaluated in terms of live fingerprints wrongly classified as fake ones (false reject rate, FRR) and fake fingerprints wrongly classified as alive ones (false accept rate, FAR). In a practical use of this measure, D_T and D_V are data sets available to the designer, which computes the radius value maximising the Fisher distance with D_T, and estimates the classification threshold for an expected error rate with D_V (e.g. the EER threshold). Once the radius and the threshold have been set, the fingerprint vitality detector is online and can classify unknown images submitted in a real operative environment (in our experiments this is "represented" by images in D_X). We repeated the above performance assessment for 500 random permutations of the data in D in order to get different partitions, and reported the average and the standard deviation for these runs in Table 6.1. In all runs the sizes of D_T, D_V, D_X were 640, 320, 480 samples, respectively. The priors of fake and live classes were equal. It is easy to see from Table 6.1 that the radius values are very stable around their average. Accordingly, estimating the radius by using the class-separation metric on a training set, namely, the Fisher distance, is effective. Error rate results further show the effectiveness of the proposed measure. In particular, the standard deviation of the expected EER is very near to its mean. The correspondent FAR and FRR follow the prediction on D_V, also by exhibiting a low standard deviation.

	Average	**Standard deviation**
Radius (freq. units)	133	4
EER (%)	2.4	0.9
FAR (%)	2.0	0.9
FRR (%)	3.3	2.1

Table 6.1: Average and standard deviation values of the Radius on D, the expected EER on D, the related error rate on D_X, for the 500 runs of our experiment. error rate on D_X, for the 500 runs of our experiment.

6.6 Performance comparison

In order to assess the performance of the proposed morphologic features we propose a comparison of the live-fake classification accuracy of these with the features of the state-of the-art. All the proposed results are based on the dataset described at Section 6.4.

Table 6.2 shows the best accuracy obtained with the proposed methods, the analogue global measure we adopted in [58] and the set of state-of-the-art features also used in that paper [53], [54], [56]. We have tuned the parameters of the new features in order to consider the best-case selection: concerning with the ridge width liveness detection method, we have considered a mask with a radius of 200 pixels and 32 sectors (for the classification we have excluded the inner eight sectors). Instead, for the computation of power spectrum we have fixed the integration area with a frequency radius of 100 frequency units. The other features from the previous works do not need a parameter selection. The second column of Table 6.2 is related to the percentage of patterns correctly classified, the third one

to the percentage of fake fingerprints correctly detected (fake detection rate), and the fourth one to the percentage of live fingerprints wrongly classified as fake ones (live misdetection rate). An evident observation it that both the new approaches allow a performance much better than that of the state-of-the-art features. Moreover, these exhibit a good trade-off between fake detection rate and live misdetection rate. In other words, the rate of clients (genuine users) ”stopped” by a false positive message in real operative environments should be significantly lower than that exhibited by other features. The only feature having a lower live misdetection rate, that is, the perspiration-based feature proposed in [56], exhibits a very low fake detection rate (Table 6.2, sixth row). In other words, it has a negligible impact on fraudulent access trials by fake fingerprints. Eighth row of Table 6.2 also points out that our features exhibit a performance superior than that of all investigated state-of-the-art features. The overall performance difference is greater than 3.0%. Even in this case, the live misdetection rate of the proposed method is the lowest one.

The last two rows are related to the fusion of new features. Applying a classification directly in the feature space allows to obtain the best accuracy. This result is allowed by the complementarity of the two morphologic features. The fusion of the new measures by an arithmetic average gives a less significant performance than the previous combination procedure but greater if compared with the other methods. On the basis of reported results, we believe the our work can be considered an effective contribution for detecting the vitality of fingerprint images.

Feature	**Overall Accuracy**	**Fake detect. rate**	**Live mis-detect. rate**
Ridge Width	81.3	81.1	18.4
Power Spectrum	84.4	85.1	16.4
Ridge width (SF3 in [58])	68.7	69.2	31.7
DM3 [53], [56]; DF1 [58]	62.2	63.1	38.7
DM5 [10]; DF2 [58]	49.4	50.8	52.0
DM6 [10]; DF3 [58]	51.4	8.9	3.6
Bending energy [54]; SF2 in [58]	48.5	49.9	52.7
Fusion (Old feature space)	78.7	79.0	21.6
Fusion (New feature space)	92.9	93.6	7.9
Fusion (Arithmetic Average new features)	90.3	90.8	10.2

Table 6.2: Percentage accuracy of the proposed measures compared with that of the state-of-the-art features [53], [54], [56]. The column ”fake detection rate” is related to the rate of fake fingerprints correctly detected, whilst the column ”live misdetection rate” is related to the rate of live fingerprints wrongly classified as fake ones.

Concluding remarks

A biometric system is a recent technology that permits the automatic recognition of an individual by some of his physics or behavioural marks. The development and diffusion of such systems has driven a particular attention toward high performance and security. Concerning on this last design bond, a considerable number of recent works have focused the attention on the wide spread of threats that can compromise a biometric system. After a brief introduction on the born of such technology, we have given a detailed description and classification of all the weak points of an automatic process of identification. In particular, the entire work of this thesis has dwelled upon one of these threats: fake biometric. A spoof attack involves the use of a fake biometric (fingerprint, for our work) to imitate a legitimate submission. From the first studies in 2002 (the well publicized study of Matsumoto) to the current researches, academic and industrial groups have tested the vulnerability of commercial fingerprint scanner showing how it is possible the reproduction of a fingerprint and the use of this for a ”spoofing” attack. If on one hand, the first works have shown the feasibility of submitting a fake fingerprint, currently the attention is focused on developing solution against such threats. ”Liveness detection” is the expression with which is indicated the research of a vitality sign in the submitted biometric, in order to avoid and obstruct

deceitful attempts. Although the research in this field is quite recent, a lot of solutions have been proposed: from hardware ones, based on the integration in the biometric system of an additional device devoted to liveness detection, to software solutions that manage the task by algorithms for digital image. In both cases, the variety of solutions is not supported by testing procedures. All the features are analyzed on limited dataset of images that does not guarantee statistical validity.
Our work is oriented toward two main direction: firstly, we have organized the state of the art in a clear taxonomy, classifying all the solutions by means of their typology (elastic deformation, morphologic features...) and by their measure protocol (dynamic, static...). Secondly, we have implemented liveness detection methods proposed in literature and proposed new ones: after having reproduced all the main measures of the state-of-the-art we have applied these on a statistical valid dataset. We have,so, analyzed the classification accuracy of such measures and their fusion on this new set of images. From this study we have found that, in order to obtain high performance, it is suggested to employ the fusion of different typologies of measures, exploiting their orthogonality. Higher classification accuracy is obtained with two novel morphologic features presented in the last chapter. The first based on the measure of the ridge width alteration, the second on the high frequency contribution in the Fourier space. Our work gives an important contribution in the liveness detection method because, after defining a clear state-of-the-art, proposes new valid solutions in this field. Although the high efforts for obtaining more and more efficient liveness detection measures, the research is still in an early state. The novelty of the question has had the upper hand on the strictness of the experimental results. Currently, the integration of liveness detection methods in a real biometric systems remains one fundamental task for

future works: that is how it is possible the combination of a verification systems with the liveness detection modulus and how the performance of such systems can be altered with the increase of security levels.

Bibliography

[1] W. Zhao, R. Chellappa, A. Rosenfeld, and P. J. Phillips, *Face Recognition: A Literature Survey*, UMD CfAR Technical Report CAR-TR948.

[2] R. Chellappa, C.L. Wilson, and S. Sirohey, *Human and machine recognition of faces: a survey*, Proceedings of the IEEE, Vol. 83, pp. 705-741, May 1995.

[3] J. Kittler, A. Hilton, M. Hamouz, J. Illingworth, *3D Assisted Face Recognition: A Survey of 3D Imaging* , Computer Vision and Pattern Recognition, 2005 IEEE Computer Society , 20-26 June 2005, 3, 114.

[4] D. A. Socolinsky, and A. Selinger, *A Comparative Analysis of Face Recogntion Performance with Visible and Thermal Infrared Imagery"* Proceedings of ICPR, pp. 217-222, 2002.

[5] Evans, David C., *Infrared facial recognition technology being pushed toward emerging applications*, 25th AIPR Workshop: Emerging Applications of Computer Vision, Vol. 2962, p. 276-286.

[6] Mark Burge, Wilhelm Burger, *Ear Biometrics in Computer Vision*, 15th International Conference on Pattern Recognition (ICPR'00) - Volume 2, 2000, p. 2822.

[7] Ping Yan, Kevin W. Bowyer, *Biometric Recognition Using 3D Ear Shape*, IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 29, no. 8, pp. 1297-1308, Aug., 2007.

[8] R. Sanchez-Reillo, C. Sanchez-Avila, A. Gonzalez-Marcos, *Biometric identification through hand geometry measurements*, Transactions on Pattern Analysis and Machine Intelligence ,Oct 2000, 22, 1168- 1171.

[9] R. B. Hill, *Retina Identification*, Biometrics: Personal Identification in Networked Society, by Anil Jain, Ruud Bolle, and Sharath Pankati, p. 126.

[10] R. B. Hill, *Apparatus and method for identifying individuals through their retinal vasculature patterns*, US Patent No. 4109237, 1978.

[11] R. Wildes, *Iris recognition: An emerging biometric technology*, Proc. IEEE, 85:1348–1363, 1997.

[12] S. V. Stevenage, M. S. Nixon and K. Vince, *Visual Analysis of Gait as a Cue to Identity*, Applied Cognitive Psychology, 13(6), pp 513-526, 1999.

[13] J. Little and J. Boyd, *Recognising People by Their Gait: the Shape of Motion*, Videre, 14(6), pp 83-105, 1998.

[14] N. Wada, S. Hangai, *HMM Based Signature Identification System Robust to Changes of Signatures with Time*, 2007 IEEE Workshop on Automatic Identification Advanced Technologies, 7-8 June 2007, 238-241.

[15] D. Hosseinzadeh, S. Krishnan, A. Khademi, *Keystroke Identification Based on Gaussian Mixture Models*, 2006 IEEE International Conference on Acoustics, Speech and Signal Processing, 2006, Volume 3, Issue , 14-19 May 2006 Page(s):III - III.

[16] E. R. Henry, *Classification and uses of Finger Prints*, London:Routledge, 1900.

[17] Biometrics Market and Industry Report 2007/2012, International Biometric Group.

[18] H. Lee and R.E. Gaensslen, *Advances in fingerprint technology* , CRC Press, 2nd ed. 2001

[19] Third International Competition for Fingerprint Verification Algorithm, FVC2004.

[20] D. Maltoni, D. Maio, A.K. Jain, S. Prabhakar, *Handbook of fingerprint recognition*, Springer, New York 2003.

[21] IBG BioPrivacy Initiative site, *http://www.bioprivacy.org/best_practices_main.htm.*

[22] Decreto legislativo 30 giugno 2003, n.196.

[23] La videosorveglianza e la biometria, Relazione 2006 - l'attività svolta dal Garante - 12 luglio 2007.

[24] Chris Roberts, *Biometric attack vectors and defences*, Computer & Security, 26(1) 14-25, 2007.

[25] R. Cappelli, D. Maio, A. Lumini, D. Maltoni, *Fingerprint image reconstruction from standard templates*, Pattern Analysis and Machine Intelligence, vol. 29 (9), 1489-1503, september 2007.

[26] A. Adler, *Can images be regenerated from biometric templates*, Proc. Biometrics Consortium Conf., Sept. 2003.

[27] Int'l Biometric Group *Generating images from templates*, white paper, IBG, 2002.

[28] L. Thaleim, J. Krissler, *Body Check: Biometric Access Protection Devices and their Program to put the test*, c't magazine, November 2002.

[29] H. Chen, H. Valizadegan, C. Jackson, S. Soltysiak and A. K. Jain, *Fake Hands: Spoofing hand geometry systems*, Biometric Consortium 2005, Washington DC, September 2005.

[30] G. Pan, L. Siu, Z. Wu, S. Lao, *Eyeblink-based anti-spoofing in face recognition from generic web-camera*, The 11th IEEE International Conference on Computer Vision (ICCV07), Rio de Janeiro, Brazil, October 14-30. To appear.

[31] Arthur Conan Doyle, *The return of Shrlock Holmes*, George Newnes, 1905.

[32] R. Austen Freeman, *The Read thumb mark*, Dr Thorndyke series, 1907.

[33] S. A. Cole, *Suspect Identitites A History of Fingerprinting and Criminal Identification*. Harvard University Press, Cambridge, Massachusetts, London, England, 2001.

[34] David Wills, Mike Lee, *Six biometric devices point the finger at security*, Network Computing, June 1,1998.

[35] T. van der Putte, J. Keuning, *Biometrical fingerprint recognition: dont get your fingers burned*, In Proceedings of IFIP TC8/WG8.8 4th Working Conference on Smart card Research and Advanced Applications, pp. 289-303, Kluwer Academic Publisher, September 2000.

[36] T. Matsumoto, H. Matsumoto, K. Yamada e S.Hoshino, *Impact of artificial gummy fingers on fingerprint systems*, In Proceedings of SPIE Vol. 4677, Optical Security and Counterfeit Deterence Techniques IV, Yokohama, Japan, January 2002.

[37] L. Thalheim, J. Krissler and P-M Ziegler, *Body check Biometric Access protection devices and their programs put to the test*, ct magazine, May 2002

[38] A. Ligon, *An investigation into the vulnerability of the Siemens id mouse Professional Version 4*, September 2002. Available at http://www.bromba.com/knowhow/idm4vul.htm.

[39] A. Stén, A. Kaseva, and T. Virtanen, *Fooling fingerprint scanners - biometric vulnerabilities of the preciseTMbiometrics 100 sc scanner*, In 4th Australian Information Warfare and IT Security Conference 2003, Helsinki, Finland, 2003.Telecommunication Software and Multimedia Laboratory, Helsinki University of Technology.

[40] Ann Harrison, *Hackers claim new fingerprint biometric attack*, SecurityFocus, 13 August 2003.

[41] J. Blommé, *Evaluation of biometric security systems against artificial finger*, Masters Thesis, Linkoping, October 2003.

[42] S. A. C. Schuckers, *Spoofing and anti-spoofing measures*, Information Security Technical Report, 7(4):5662, December 2002.

[43] M. Sandstrom, *Liveness detection in fingerprint recognition systems*, Masters Thesis, Linkoping, June 2004.

[44] P. Lapsley, J. Less, D. Pare, N. Hoffman, Anti-Fraud Biometric Sensor that Accurately Detects Blood Flow, SmartTouch, LLC, US Patent 5,737,439, (1998).

[45] Kristin A. Nixon, Robert K. Rowe, *Multispectral fingerprint imaging for spoof detection*, Proc. SPIE, Vol. 5779, 214-225, Biometric Technology for Human Identification II.

[46] L. Biel, O. Pettersson, L. Philipson, P. Wide, *ECG analysis: A new approach in human identification*, IEEE Transactions on Instrumentation and Measurement 50 (3) 808-812 (2001).

[47] D. Baldissera, A. Franco, D. Maio, D. Maltoni, *Fake Fingerprint Detection by Odor Analysis*, in proceedings International Conference on Biometric Authentication (ICBA06), Hong Kong, January (2006).

[48] G. Parziale, *Touchless fingerprint technology*, a chapter in *Advanced in Biometrics: Sensors, Systems and Algorithms*, Ed. by Nalini K. Ratha and Venu Govundaju, Springer-Verlag Ltd, 2008.

[49] G. Parziale *Advanced 3D Touchless Fingerprinting*, 3rd Summer School on Biometrics, June 5-10,2006, Alghero, Italy.

[50] A. Jain, Y. Chen, M. Demirkus, *Pores and Ridges: Fingerprint macthing using level 3 features*, IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 29, no. 1, pp. 15-27, Jan. 2007.

[51] D. Osten, H.M. Carim, M.R. Arneson, and B. L. Blan, Biometric, Personal Authentication System, U.S. Patent 5 719 950, Feb. 17, (1998).

[52] A.K. Jain, R. Bolle and S. Pankanti (Eds.), *BIOMETRICS: Personal Identification in Networked society*, Kluwer Academic Publishers, (1999).

[53] R. Derakhshani, S. Schuckers, L. Hornak , L. O'Gorman, *Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners*, Pattern Recognition 36 (2) (2003) 383-396.

[54] Y. Chen, A.K. Jain, S. Dass, *Fingerprint deformation for spoof detection*, Biometric Symposium, Cristal City, VA, (2005).

[55] Y.S. Moon, J.S., Chen, K.C. Chan, K. So, K.C. Woo, *Wavelet based fingerprint liveness detection*, Electronics Letters, 41 (20) (2005) 1112-1113.

[56] S. Parthasaradhi, R. Derakhshani, L. Hornak, S. Schuckers, *Time-series detection of perspiration as a vitality test in fingerprint devices*, IEEE Trans. On Systems, Man and Cybernetics, Part C, 35 (3) (2005) 335-343.

[57] A. Antonelli, R. Cappelli, D. Maio, D. Maltoni, *Fake Finger Detection by Skin Distortion Analysis*, IEEE Transactions on Information Forensics and Security, Vol.1, no.3, (2006) 360-373.

[58] P. Coli, G.L. Marcialis, F. Roli, *Analysis and selection of feature for the fingerprint vitality detection*, SSPR/SPR 2006 (2006) 907-915.

[59] B. Tan, S. Schuckers, *Liveness detection for fingerprint scanners based on the statistics of wavelet signal processing*, Conference on Computer Vision Pattern Recognition Workshop (CVPRW06), (2006).

[60] P. Coli, G.L. Marcialis, F. Roli, *Vitality detection from fingerprint images: a critical survey*, 2nd International Conference on Biometrics ICB 2007, vol. 4642, Seoul (South Korea), Springer, pp. 722-731.

[61] J. Galbally, J. Fierrez, J. D. Rodriguez-Gonzalez, F. Alonso-Fernandez, Javier Ortega-Garcia, and M. Tapiador, *On the vulnerability of fingerprint verification systems to fake fingerprints attacks*, Proc. 40th International Carnahan Conference on Security Technology, ICCST, pp. 130-136, October 2006.

[62] S. Prabhakar, A.K. Jain, *Decision-level Fusion in Fingerprint Verification*, Pattern Recognition, 35 (4) 861-874, 2002.

[63] A. Ross, S. Dass, A.K. Jain, *A deformable model for fingerprint matching*, Pattern Recognition, 38 95-103, 2005.

[64] S. Raudys, A.K. Jain, *Small Sample Size Effects in Statistical Pattern Recognition: Recommendations for Practitioners*, IEEE Trans. PAMI, 13 (3) 252-264, 1991.

[65] D. Maio, D. Maltoni, R. Cappelli, J.L. Wayman, A.K. Jain: FVC2004: Third Fingerprint Verification Competition. ICBA (2004): 1-7.

[66] web site, *http://www.biometricgroup.com/spoof*.

[67] E. Tabassi, C.L. Wilson, C.I. Watson, *Fingerprint image quality*, NIST Technical Report NISTIR 7151, August, 2004.

[68] Pietro Coli, Gian Luca Marcialis, Fabio Roli, *Power spectrum-based fingerprint vitality detection*, IEEE Workshop on Automatic Identification Advanced Technologies AutoID 2007, 2007 .

[69] A.K. Jain, S. Prabhakar, L. Hong, S. Pankati, *FingerCode: A filterbank for fingerprint representation and matching*, Proc. Of IEEE CVPR, Vol. 2, pp. 187-193 (1999).

[70] L. O'Gorman and J.V. Nickerson, *An approach to fingerprint filter design*, Pattern Recognition, vol. 22, no. 1, pp.29-38.

[71] Y. Yin, J. Tian, X. Yang, *Ridge Distance Estimation in Fingerprint Images: Algorithm and Performance Evaluation*, EURASIP Journal on Applied Signal Processing, vol. 2004, no. 4, pp. 495-502, 2004.

[72] A. K. Jain, S. Prabhakar, L. Hong, S. Pankanti, *FingerCode: A Filterbank for Fingerprint Representation and Matching*, cvpr, p. 2187, 1999 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'99) - Volume 2, 1999.